2/2017

Datenschutz Nachrichten

40. Jahrgang
ISSN 0137-7767
12,00 Euro



BDSG-neu und andere Baustellen

■ Das neue Datenschutzgesetz ■ Verfassungswidrige Beschränkung der Datenschutzkontrolle bei Berufsgeheimnisträgern ■ Beschäftigtendatenschutz nach der DS-GVO und nach dem BDSG-neu ■ Türkische Geheimdiensttätigkeit in Deutschland ■ BigBrotherAwards 2017 ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Samstag, 09. September 2017
„Freiheit 4.0 - Rettet die Grundrechte“ Demo
Berlin

Sonntag, 17. September 2017
DVD-Vorstandssitzung
Kiel, Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Montag, 18. September 2017
Sommerakademie 2017, Kiel
https://www.datenschutzzentrum.de/sommerakademie/2017/

Samstag, 21. Oktober .2017
DVD-Vorstandssitzung
Bonn, Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 22.10.2017
DVD-Mitgliederversammlung 2017
Bonn

Mittwoch, 01. November 2017
Redaktionsschluss DANA 4/2017

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
40. Jahrgang, Heft 2

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Werner Hülsmann
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Copyright
Die Urheber- und Vervielfältigungsrechte liegen bei den Autoren. Der Nachdruck ist nach Genehmigung durch die Redaktion bei Zusendung von zwei Belegexemplaren nicht nur gestattet, sondern durchaus erwünscht, wenn auf die DANA als Quelle hingewiesen wird.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta,
Sternhimmel Titelbild: NASA

Editorial

Nun ist es da, das neue Bundesdatenschutzgesetz. Als Artikel 1 des DSAnpUG-EU ist es am 05.07.2017 im Bundesgesetzblatt veröffentlicht worden. In dieser DANA-Ausgabe widmen sich gleich drei Artikel dem BDSG-neu: Ein allgemeiner Artikel zum BDSG-neu, der Artikel „Verfassungswidrige Beschränkung der Datenschutzkontrolle bei Berufsgeheimnisträgern“ sowie ein Artikel zum Beschäftigtendatenschutz.

Artikel zu unterschiedlichen Aspekten der Datenschutzgrundverordnung dürfen natürlich auch nicht fehlen.

Die Aktivitäten des türkischen Geheimdienstes in Deutschland beleuchtet ein Artikel auch unter Datenschutzgesichtspunkten. Neben den traditionellen Datenschutzschutznachrichten und Buchbesprechungen gibt es noch einen bebilderten Rückblick der BigBrotherAward-Gala, die im April 2017 stattfand.

Apropos Datenkraken: Unter dem Deckmantel des harmlos klingenden „Entwurf eines Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften“ wurden zum einen bei verschiedenen Gesetzen die erforderlichen Anpassungen vorgenommen. Zum anderen wurden mit diesem sogenannten Omnibusgesetz gleich mehrere aus Datenschutzgesichtspunkten sehr bedenkliche Gesetzesänderungen verabschiedet. Hierzu gehören u.a. die Schaffung einer umfassenden Befugnis zur Nutzung automatisierter Fingerabdruck-Scans von Asylsuchenden ohne irgendwelche Sicherungsmaßnahmen, die Änderung der Zuständigkeit für die Datenschutzaufsicht im Steuerbereich von den Ländern hin zum Bund und die Beschränkung des Auskunftsanspruchs der Bürgerinnen und Bürger gegenüber der Steuerverwaltung. Die entsprechenden Änderungen des ursprünglichen Gesetzentwurfs wurden in einer 139-seitigen Ausschussdrucksache untergebracht, die am Tag nach der entscheidenden Ausschusssitzung vom Bundestag beschlossen wurde. Da hatte selbst die interessierte Fachöffentlichkeit kaum die Möglichkeit, sich kritisch mit den Änderungen auseinander zu setzen. Eine Vorabversion der Ausschussdrucksache diente der Erstellung unserer Pressemitteilung vom 30.05.2017. Die Einführung des Staatstrojaners ist uns zwar nicht entgangen, aber unserer Ressourcen ließen es leider nicht zu, hierzu eine Pressemitteilung zu verfassen. Auch hier wurden gravierende Änderungen erst kurz vor der Beschlussfassung im Bundestag in den Entwurf aufgenommen. Der Staatstrojaner war im ursprünglichen Gesetzentwurf noch nicht enthalten sondern wurde erst in der entscheidenden Ausschussdrucksache eingefügt. Transparente Gesetzgebung geht anders!

Zu befürchten ist, dass dies – egal wie die Bundestagswahl ausgehen wird – zur Methodik wird. Spannend bleibt es allemal. So sind wir auch gespannt auf das 2. DSAnpUG-EU, mit dem nach unserem derzeitigen Kenntnisstand ca. 140 Gesetze an die EU-Datenschutzgrundverordnung angepasst werden sollen.

In diesem Sinne wünschen wir Ihnen eine anregende Lektüre.

Werner Hülsmann

Autorinnen und Autoren dieser Ausgabe:

Werner Hülsmann

Vorstandsmitglied in der DVD, Mitglied des Beirats des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V., selbständiger Datenschutzberater, externer Datenschutzbeauftragter und Datenschutzsachverständiger, Ismaning und Berlin, huelsmann@datenschutzverein.de

Frans Jozef Valenta

Grafik-Designer, Vorstandsmitglied in der DVD, valenta@datenschutzverein.de

Dr. Thilo Weichert

Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise, weichert@datenschutzverein.de, Kiel

Werner Hülsmann

Das neue Bundesdatenschutzgesetz



Bild: AdobeStock

1 Einleitung

Am 25. April 2017 hat der Deutsche Bundestag in 2. und 3. Lesung den Gesetzentwurf des Datenschutzanpassungs- und -Umsetzungsgesetz EU[1] (DSAnpUG-EU, Bundestagsdrucksachen 18/11325) in der Fassung der Beschlussempfehlung des Innenausschusses (Bundestagsdrucksache 18/12084) beschlossen. Diesem Gesetzesbeschluss hat der Bundesrat am 12. Mai 2017 zugestimmt. Am 05. Juli 2017 erfolgte die Verkündung des DSAnpUG-EU im Bundesgesetzblatt[2], es tritt – mit Ausnahme des Art. 7 des DSAnpUG-EU gleichzeitig mit dem Wirksamwerden der EU-Datenschutzgrundverordnung (DS-GVO) am 25. Mai 2018 in Kraft.

Ein wesentlicher Bestandteil des DSAnpUG-EU ist der Artikel 1, der das neue am 25. Mai 2018 in Kraft tretende Bundesdatenschutzgesetz (BDSG-neu)[3] enthält. Das derzeitige Bundesdatenschutzgesetz (BDSG-alt) tritt gemäß Art. 8 des DSAnpUG-EU am 25. Mai 2018 außer Kraft. Mit dem DSAnpUG-EU und dem darin enthaltenen BDSG-neu werden datenschutzrechtliche Regelungen an die DS-GVO angepasst, in ihr enthaltene „Öffnungsklauseln" genutzt und die „Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates" umgesetzt.

Wichtig dabei ist: Das bisherige BDSG-alt wird nicht einfach durch das BDSG-neu ersetzt. Vielmehr ersetzen die DS-GVO und das BDSG-neu gemeinsam das derzeitige BDSG-alt. Es reicht daher künftig nicht aus, nur das BDSG-neu (oder nur die DS-GVO) vor sich liegen zu haben, sondern es ist erforderlich, die Artikel der DS-GVO und die dazugehörigen Erwägungsgründe sowie die entsprechenden Paragraphen des BDSG-neu zu lesen und dies am besten übersichtlich in drei Spalten nebeneinander[4]. Allerdings sind auch weiterhin bereichsspezifische Regelungen, auch auf europäischer Ebene – wie die derzeit im Entwurf befindliche ePrivacy-Verordnung[5] – zu berücksichtigen.

Grundsätzlich ist fraglich, ob alle im BDSG-neu enthaltenen Konkretisierungsregelungen durch entsprechende „Öffnungsklauseln" der DSG-VO abgedeckt sind und ob die Begründungen zur Nutzung dieser „Öffnungsklauseln" in allen Fällen ausreichend sind. Daher ist unsicher, ob alle derzeit im BDSG-neu enthaltenen Vorschriften aus europarechtlicher Sicht Bestand haben können.

2 Für wen gilt das BDSG-neu?

Das neue Bundesdatenschutzgesetz (BDSG-neu) gilt gemäß § 1 BDSG-neu – wie das bisherige Bundesdatenschutzgesetz – für

- nicht-öffentliche Stellen (wie Firmen, Vereine, Stiftungen, Einzelunternehmer, Selbständige, Freiberufler)
- öffentliche Stellen der Länder, sofern in dem Bundesland der Datenschutz nicht durch Landesgesetz geregelt ist (das kommt in der Praxis nicht vor)
- öffentliche Stellen des Bundes.

Bereichsspezifische Regelungen gehen allerdings nach wie vor denen des BDSG-neu vor. Sofern einzelne Regelungen des BDSG-neu, die im Anwendungsbereich der DS-GVO gelten sollen (das sind die Teile 1 und 2, s.u.) nicht mit der DS-GVO vereinbar sind, gehen die Regelungen der DS-GVO den entsprechenden Regelungen des BDSG-neu und aller anderen nationalen Gesetze vor.

3 Struktur des BDSG-neu

Das BDSG-neu besteht aus vier Teilen. Dabei sind nicht alle Teile für alle Stellen relevant.

- Teil 1 – Gemeinsame Bestimmungen (für die folgenden Teile).
- Teil 2 – Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679, das ist die DS-GVO).
- Teil 3 – Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 (also für Justiz- und Strafverfolgungsbehörden).

- Teil 4 – Besondere Bestimmungen für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten.

Für nicht-öffentliche Stellen sowie öffentliche Stellen des Bundes, die keine Behörden der Justiz oder Strafverfolgung sind, sind nur die Teile 1 und 2 relevant. Die Regelungen aus Teil 3 gelten nur für Behörden der Justiz oder Strafverfolgung (vgl. Teil 3, Kapitel 1, § 45 Anwendungsbereich BDSG-neu), für diese Behörden gelten auch noch die Paragraphen des Teils 1.

3.1 Sonderfall: Öffentliche Stellen der Länder, die am Wettbewerb teilnehmen

Ob und wie weit Regelungen der Teile 1 und 2 für die öffentlichen Stellen der Länder gelten, die am Wettbewerb teilnehmen, ist von den entsprechenden noch anzupassenden Landesdatenschutzgesetzen abhängig. So gibt es bisher einige Landesdatenschutzgesetze, in denen für öffentliche Stellen dieser Länder, die am Wettbewerb teilnehmen, ganz allgemein auf die Regelungen des BDSG für nicht-öffentliche Stellen verwiesen wird. Derartige Verweise funktionieren auch mit dem BDSG-neu, andere Landesdatenschutzgesetze verweisen auf einzelne Abschnitte oder Paragraphen des BDSG-alt. Diese Verweise funktionieren nicht mehr mit dem BDSG-neu und sind von den Landesgesetzgebern anzupassen. In einem Bundesland wird sogar explizit auf das BDSG-alt verwiesen. Hier ist unbedingt eine Anpassung vorzunehmen, da dieses BDSG am 25. Mai 2018 außer Kraft tritt.

Zum Redaktionsschluss lagen allerdings noch keine Gesetzesentwürfe zur Anpassung von Landesdatenschutzgesetzen an die DS-GVO vor.

4 Ausgewählte Regelungen des BDSG-neu

Im Folgenden werden einige ausgewählte Regelungen aus den Teilen 1 und 2 des BDSG-neu detaillierter dargestellt. Auf eine vollständige Darstellung wird aus Platzgründen an dieser Stelle verzichtet.

4.1 Teil 1 BDSG-neu

§ 1 BDSG-neu enthält den Anwendungsbereich (s.o.)

4.1.1 § 2 BDSG-neu Begriffsbestimmungen

Hier ist u.a. geregelt, was unter öffentliche Stellen des Bundes und was unter nicht-öffentliche Stellen zu verstehen ist.

„Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, der Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. “ (§ 2 Abs. 1 BDSG-neu)

Abs. 2 definiert die „öffentlichen Stellen der Länder“, Abs. 3 bestimmt, unter welchen Umständen „Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen“ als öffentliche Stellen des Bundes gelten. Abs. 4 definiert die nicht-öffentlichen Stellen:

(4) $_1$Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. $_2$Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

„Öffentliche Stellen des Bundes gelten als nicht-öffentliche Stellen im Sinne dieses Gesetzes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. “ (§ 2 Abs. 5, Satz 1 BDSG-neu).

Leider sind diese Begriffsbestimmungen nicht ganz mit der DS-GVO kompatibel, da die DS-GVO „Unternehmen“ (Art. 4, Ziff. 18) definiert und „Behörden“ sowie „öffentliche Stellen“ kennt, den Begriff „nicht-öffentliche Stellen“ aber nicht verwendet. Eine 1:1-Nutzung der Begrifflichkeiten der DS-GVO hätte hier die Anwendung erleichtert.

4.1.2 § 3 - Verarbeitung personenbezogener Daten durch öffentliche Stellen

„Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen[6] liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.“

Diese Regelung gab es grundsätzlich bereits im BDSG-alt, so dass sich an der Zulässigkeit der Datenverarbeitung durch öffentliche Stellen des Bundes durch diese Regelung nichts Wesentliches ändert.

4.1.3 § 4 BDSG-neu – Videoüberwachung öffentlich zugänglicher Räume

§ 4 Abs. 1 BDSG-neu regelt, dass eine Videoüberwachung durch Stellen nur zulässig ist,

„soweit sie

1. *zur Aufgabenerfüllung öffentlicher Stellen,*
2. *zur Wahrnehmung des Hausrechts oder*
3. *zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.“*

In § 4 Abs. 2 BDSG-neu werden „besonders wichtige Interessen“ definiert, die bei der Abwägung, ob schutzwürdige Interessen der Betroffenen überwiegen, genutzt werden sollen. Hier werden die erst vor kurzem mit dem sogenannten „Videoüberwachungsverbesserungsgesetz“ in das BDSG-alt eingefügten Vorschriften übernommen. Diese Ergänzungen des BDSG-alt sind von Datenschützer/inne/n heftig kritisiert worden.

Da mangels „Öffnungsklausel“ in der DS-GVO berechtige Zweifel an der europarechtlichen Zulässigkeit dieser Regelungen bestehen, sollte sich für die Einschätzung der datenschutzrechtlichen Zulässigkeit von Videoüberwachungsmaßnahmen in erster Linie an Art. 6 DS-GVO – insbesondere Buchst. e (für öffentliche Stellen: Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt) und f (für nichtöffentliche Stellen: Interessenabwägung) – orientiert werden.

4.1.4 Kapitel 5, §17 Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle

Die Beschränkung der Zuständigkeit der aus dem Kreis der Datenschutz-Aufsichtsbehörden der Länder gewählte Stellvertretung im Europäischen Datenschutzausschuss (EDSA) auf „Angelegenheiten, die die Wahrnehmung einer Aufgabe betreffen, für welche die Länder alleine das Recht zur Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen" ist nicht zielführend, da die/der BfDI nur für die Kontrolle von Unternehmen, die Post- oder Telekommunikationsdienstleistungen erbringen, zuständig ist und in allen anderen die Unternehmen betreffenden Fragestellungen bisher weder zuständig ist noch entsprechende Erfahrungen sammeln konnte. Für eine kompetente Vertretung der Datenschutz-Aufsichtsbehörden, die auch für die Unternehmen aus der Finanzbranche zuständig sind, im EDSA wäre es daher – auch für die betroffenen Institute – besser, wenn die Stellvertretung auch für diese Themen im EDSA zuständig wäre.

4.1.5 Kapitel 6, § 21 - Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission

Diese Regelung ermöglicht es den Datenschutz-Aufsichtsbehörden direkt gegen Angemessenheitsbeschlüsse der EU-Kommission sowie gegen Beschlüsse über die Allgemeingültigkeit von genehmigten Verhaltensregelungen vorzugehen, sofern diese für eine Entscheidung einer Aufsichtsbehörde – z.B. im Rahmen einer Datenschutz-Kontrolle – relevant sind. Eine solche Regelung war längst überflüssig und ist mit Artikel 7 des DSAnpUG-EU auch in das aktuelle BDSG als § 42b mit Wirkung zum 06. Juli 2017 eingefügt worden. Es bleibt abzuwarten, wann die erste Aufsichtsbehörde dieses Mittel z.B. im Zusammenhang mit den Standard-Vertragsklauseln oder dem EU-US Privacy Shield nutzt.

4.2 Teil 2 - Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 2 der Verordnung (EU) 2016/679

4.2.1 Kapitel 1, Abschnitt 1 - Verarbeitung besonderer Kategorien personenbezogener Daten und Verarbeitung zu anderen Zwecken

In diesem Abschnitt werden zum einen durch § 22 BDSG-neu weitere – über die in Art. 9 DS-GVO enthaltenen – Ausnahmen vom dortigen Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten eingefügt. Diese zusätzlichen Ausnahmen sind grundsätzlich durch die „Öffnungsklauseln" des Art. 9 DS-GVO abgedeckt.

Zum anderen werden in den §§ 23 und 24 BDSG-neu weitere Möglichkeiten zur Zweckänderung – auch in Bezug auf besonderer Kategorien personenbezogener Daten – für öffentliche und nicht-öffentliche Stellen geschaffen, sowie in § 25 BDSG-neu die Übermittlung personenbezogener Daten von öffentlichen Stellen an andere öffentliche Stellen und an nicht-öffentliche Stellen geregelt. Diese Regelungen stellen eine sehr weitgehende Ausnutzung der „Öffnungsklauseln" dar und sollten daher von den verantwortlichen Stellen „im Lichte der DS-GVO" interpretiert werden.

4.2.2 Kapitel 1, Abschnitt 2 - Besondere Verarbeitungssituationen

Dieser Abschnitt enthält unter anderem zwei Paragraphen, denen in dieser DANA-Ausgabe jeweils ein eigenständiger Artikel gewidmet ist. Zum § 26 *Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses* BDSG-neu siehe „Beschäftigtendatenschutz nach der DS-GVO und dem BDSG-neu" und zum § 29 *Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten* BDSG-neu siehe „Verfassungswidrige Beschränkung der Datenschutzkontrolle bei Berufsgeheimnisträgern".

§ 30 *Verbraucherkredite* BDSG-neu übernimmt 1:1 die Regelungen aus § 29 Abs. 6 und 7 BDSG-alt, die der Umsetzung der EU-Verbraucherkreditrichtlinie dienen.

§ 31 *Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften* BDSG-neu übernimmt zum einen die Regelungen aus § 28b *Scoring* BDSG-alt und regelt zum anderen – in Anlehnung an die entsprechenden Regelungen aus § 28a *Datenübermittlung an Auskunfteien* BDSG-alt – die Befugnisse zur Verwendung der von Auskunfteien übermittelten Wahrscheinlichkeitswerte über die Zahlungsfähig- und Zahlungswilligkeit von natürlichen Personen. Die Übernahme dieser Regelungen aus dem alten in das neue BDSG wird von Verbraucherschutz- und Wirtschaftsverbänden, wie auch von einem großen Teil der Datenschutz-Aufsichtsbehörden begrüßt. Es ist allerdings zweifelhaft, ob derartige Regelungen im öffentlichen Interesse erforderlich und daher noch mit den Öffnungsklauseln der DS-GVO zu vereinbaren sind.

4.3 Kapitel 2 Rechte der betroffenen Person

Eigentlich müsste hier – angesichts der in diesem Kapitel enthaltenen Vorschriften – die Überschrift lauten: „Einschränkungen der Rechte der betroffenen Person". Hier sind Regelungen enthalten, die deutliche Einschränkungen der Rechte der betroffenen Personen vorsehen. Diese Einschränkungen der Betroffenenrechte gehen weit über das hinaus, was durch die DS-GVO an Beschränkungen zugelassen wird. Daher gilt auch hier: Diese Paragraphen sind ebenfalls „im Lichte der DS-GVO" auszulegen. Es ist zudem davon auszugehen, dass einige der Vorschriften keinen dauerhaften Bestand haben werden.

§ 37 *Automatisierte Entscheidungen im Einzelfall einschließlich Profiling*

Die im § 37 BDSG-neu aufgeführte zusätzliche Ausnahme vom Verbot automatisierter Einzelfallentscheidungen gilt nur für die Leistungserbringung nach einem Versicherungsvertrag und wird hier nicht weiter ausgeführt.

Kapitel 3 - § 38 - *Datenschutzbeauftragte nicht-öffentlicher Stellen*

Mit § 38 BDSG-neu wird die bewährte Regelung des § 4f BDSG-alt übernommen, so dass verantwortliche Stellen und Auftragsverarbeiter auch dann eine/n Datenschutzbeauftragte/n verpflichtend zu benennen haben, wenn sie „in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäfti-

gen". Darüber hinaus ist auch dann ein/e Datenschutzbeauftragter/r zu bennenen, wenn die verantwortliche Stelle oder der Auftragsverarbeiter Verarbeitungen vornehmen, für die eine Datenschutz-Folgenabschätzungen nach Art. 35 DS-GVO vorzunehmen ist. Diese Vorschriften nutzen die „Öffnungsklausel" aus Art. 37 Abs. 4 DS-GVO.

§ 38 Abs. 2 BDSG-neu verweist auf Vorschriften zu den Datenschutzbeauftragten für öffentliche Stellen (§ 6 Abs. 4, Abs. 5 Satz 2 und Abs. 6 BDSG-neu).

§ 6 Abs. 4 gilt dabei nur für Datenschutzbeauftragte, deren Benennung nach EU- oder nationalem Recht verpflichtend ist. Dieser Absatz schützt – wie bisher § 4f Abs. 3 Satz 4ff – die verpflichtend benannten Datenschutzbeauftragten vor willkürlicher Abberufung und – sofern es sich um Angestellte der verantwortlichen Stelle oder des Auftragsverarbeiters handelt – vor willkürlicher Kündigung. Auch wenn die Übernahme dieser Vorschrift sehr zu begrüßen ist, ist fraglich, ob diese Vorschrift sich noch im Rahmen der „Öffnungsklausel" aus Art. 37 Abs. 4 DS-GVO bewegt oder – insbesondere der Kündigungsschutz – in den Regelungsbereich des keine „Öffnungsklausel" enthaltenden Art. 38 DS-GVO zur Stellung des Datenschutzbeauftragten fällt (vgl. Art. 38 Abs. 3 zum Benachteiligungsverbot) und somit aus EU-rechtlicher Sicht unzulässig ist.

§ 6 Abs. 5 Satz 2 BDSG-neu übernimmt in Nutzung der „Öffnungsklausel" aus Art. 38 Abs. 5 DS-GVO die aus § 4f Abs. 4 BDSG-alt bekannte Verschwiegenheitsverpflichtung über die Identität der betroffenen Person, die sich an den/die Datenschutzbeauftragte/n gewandt hat.

Unabhängig von einer Benennungspflicht eines/einer Datenschutzbeauftragten muss es in jedem Unternehmen unabhängig von der Größe des Unternehmens mindestens eine Person geben, die auf die Einhaltung der datenschutzrechtlichen Verpflichtungen achtet. Zwar ist das Datenschutzmanagement eine Aufgabe, für die der Vorstand oder die Geschäftsführung grundsätzlich verantwortlich ist. Allerdings ist die konkrete Umsetzung dieser Aufgaben bei den Datenschutzbeauftragten gut aufgehoben. Zwar sieht die DS-GVO vor, dass Unternehmen auch auf freiwilliger Basis betriebliche Datenschutzbeauftragte benennen dürfen. Ob dies allerdings bei den Unternehmen in größerem Umfang erfolgen würde, ist sehr fraglich. Zur Wahrung der Grundrechte und der Grundfreiheiten der betroffenen Personen aber auch aus Unternehmenssicht (nämlich zur Reduzierung von Bußgeldrisiken für die Unternehmen) ist es daher zu begrüßen, dass viele Unternehmen durch die in § 38 Abs. 1 BDSG-neu enthaltenen Vorschriften weiterhin zu „ihrem Glück gezwungen" werden.

5 Kritik am neuen Bundesdatenschutzgesetz

Bereits die Gesetzentwürfe für das DSAnpUG-EU mit dem neuem BDSG haben viel Kritik hervorgerufen. Zu den Kritikpunkten der DVD gehörten insbesondere[7]:

- Die geplante Regelung zur Videoüberwachung mit der Vorrangregelung für öffentliche Sicherheitsbelange ist europa- und verfassungswidrig.
- Die Regelung zur Bestellung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) verstößt hinsichtlich der geforderten Transparenz und den personellen Anforderungen gegen die europarechtlichen Vorgaben.
- Die eingeschränkten Kontroll- und Sanktionsmöglichkeiten der BfDI im öffentlichen und insbesondere im Sicherheitsbereich untergraben insofern die Effektivität der Datenschutzaufsicht.
- Die Regelungen zur Vertretung der Aufsichtsbehörden der Länder im Europäischen Datenschutzausschuss beeinträchtigen deren Unabhängigkeit.
- Die Einschränkung der Kontrollbefugnisse der Datenschutzaufsicht im Bereich der Berufsgeheimnisse ist nicht akzeptabel.
- Die Möglichkeiten zur Verweigerung von Auskünften an Betroffene sind zu unbestimmt und zu weitgehend.
- Es verbleiben große Regelungsdefizite in Bezug auf die Datenverarbeitung in Beschäftigungsverhältnissen, der Forschung, der Beauftragung von IT-Dienstleistern sowie des Angebots von Herstellern und Anbietern von IT-Produkten.

Weitere Kritikpunkte wurden von den Datenschutzbeauftragten der Länder und von weiteren Institutionen geäußert.

Auf einige wenige Kritikpunkte wurde im Gesetzgebungsverfahren noch reagiert. Die wesentlichen Kritikpunkte der DVD und anderer Datenschutzverbände blieben allerdings unberücksichtigt[8].

6 Fazit

Auch wenn es grundsätzlich zu begrüßen ist, dass etwa ein Jahr vor dem Gültigwerden der DS-GVO die Anpassung des Bundesdatenschutzgesetzes erfolgte, gibt das BDSG-neu aber leider nicht die Rechtssicherheit, die Unternehmen und von der Datenverarbeitung betroffene Personen sich gewünscht hätten. Vielmehr ist damit zu rechnen, dass einige Regelungen nochmals geändert werden, sei es durch den Gesetzgeber (der damit EU-Vertragsverletzungsverfahren begegnen will) oder durch höchstrichterliche Rechtsprechung (auf Grund von Klagen gegen verfassungswidrige oder EU-rechtswidrige Regelungen des BDSG-neu). Es bleibt also spannend.

1 Vollständiger Name: „Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680"

2 Bundesgesetzblatt Teil I, Nr. 44, S. 2097 ff, zu finden unter https://www.bgbl.de

3 Da die kostenfreie Version des BGBl nicht druckbar ist, sei hier auf die nicht-amtliche Fassung des Autors verwiesen: https://dsgvo.expert/BDSG-neu (PDF-Datei)

4 An dieser Stelle sei auf die entsprechende Synopse des Autors verwiesen: https://efweha-verlag.de/Bd41eBook (PDF-Datei) oder als gedruckte Version: https://efweha-verlag.de/bd41

5 Vgl. hierzu die Stellungnahme der DVD zum Entwurf: https://dvd-ev.de/pm/STePrivVO (PDF-Datei und die entsprechende Pressemitteilung hierzu: https://dvd-ev.de/pm/20170531 (PDF-Datei)

6 Der in der DS-GVO und dem BDSG-neu genutzte Begriff „Verantwortliche" ersetzt den aus dem BDSG-alt bekannten bisherigen Begriff „verantwortliche Stelle". In diesem Artikel wird – aus Gründen der besseren Verständlichkeit – weiterhin der alte Begriff „verantwortliche Stelle" verwendet.

7 Vgl. Pressemitteilung der DVD vom 01.02.2017, zu finden unter https://www.datenschutzverein.de/pressemitteilungen/

8 Vgl. Pressemitteilung der DVD vom 26.04.2017, ebenfalls zu finden unter https://www.datenschutzverein.de/pressemitteilungen/

Thilo Weichert

Verfassungswidrige Beschränkung der Datenschutzkontrolle bei Berufsgeheimnisträgern

1 Abstract

Vom 25.05.2018 an tritt ein neues Bundesdatenschutzgesetz (BDSG) in Deutschland in Kraft, das den Anspruch hat, die Europäische Datenschutz-Grundverordnung (DSGVO), die von diesem Zeitpunkt an direkt anwendbar sein wird, umzusetzen. In einem § 29 Abs. 3 BDSG wird geregelt, dass die Kontrollbefugnis der Datenschutzaufsichtsbehörden im Anwendungsbereich von Berufsgeheimnissen nach § 203 StGB eingeschränkt wird. Der vorliegende Text stellt die neue Regelung vor, erörtert dessen Auslegung und kommt bei einem Abgleich mit übergeordnetem Recht zu dem Ergebnis, dass die Regelung gegen europäisches und nationales Verfassungsrecht verstößt.

2 Die Regelung

2.1 Kurze Geschichte

Am 27.04.2017 beschloss der Deutsche Bundestag in zweiter und dritter Lesung den Entwurf eines **neuen Bundesdatenschutzgesetzes** (BDSG) als Teil des Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU). Hinter diesem bürokratisch klingenden Namen verbirgt sich nichts anderes als die nationale Umsetzung der wesentlichen Vorgaben der Europäischen Datenschutz-Grundverordnung (DSGVO) und der Verordnung (EU) 2016/679. Die mediale Resonanz zu diesem für die Wahrung der digitalen Grundrechte in Europa wichtigen Gesetz tendierte gegen Null. Auch die fachliche Resonanz hielt sich in Grenzen. Soweit es Kommentierungen gab, waren diese eher freundlich, verbunden mit dezenter Kritik, etwa des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Kritisch äußerte sich die Deutsche Vereinigung für Datenschutz e.V. (DVD) mit einer Rundumkritik. Einer von den Kritikpunkten ist: „Die Kontrollbefugnisse der **Datenschutzaufsicht im Bereich der Berufsgeheimnisse** werden bis zur Wirkungslosigkeit eingeschränkt."

Gemäß den §§ 19 Abs. 1, 40 Abs. 1 **BDSG 1977** hatten der Bundesbeauftragte für den Datenschutz sowie die Aufsichtsbehörden der Länder eine unbeschränkte Kontrollbefugnis über „die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz". Nachdem es immer wieder zu Konflikten bei der Prüfung von Stellen kam, die meinten, sich wegen ihrer besonderen Geheimhaltungspflichten der Datenschutzkontrolle entziehen zu können, wurde in § 24 Abs. 2 S. 1 **BDSG 1990** ausdrücklich klargestellt, dass sich die Kontrolle auch „auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen", erstreckt. Doch die Kontrollbefugnis blieb umstritten. Dies betraf nicht nur gesetzlich geregelte Bereiche wie die geheimdienstliche Tätigkeit, etwa im Hinblick auf die Post- und Telekommunikationsüberwachung oder Sicherheitsüberprüfungen (§ 24 Abs. 2 S. 3 **BDSG 1990**). Insbesondere Anwälte wehrten sich gegen die möglichen Prüfungen, obwohl solche in der Praxis nur in ganz wenigen Ausnahmefällen stattfanden. Widerstand kam gelegentlich auch aus dem medizinischen Bereich, wobei diese Kritik zunehmend leiser wurde, weil sich zeigte, dass mit der Datenschutzkontrolle keine Beeinträchtigung, sondern eher eine Stärkung der Arzt-Patienten-Vertraulichkeitsbeziehung einhergeht.

Nachdem nun in **Art. 90 Abs. 1 DSGVO** geregelt ist, dass die Mitgliedstaaten die Befugnisse von Datenschutzaufsichtsbehörden in Bezug auf Berufsgeheimnisse abweichend regeln dürfen, „soweit dies notwendig und verhältnismäßig ist", waren und sind Berufsverbandsvertreter wieder animiert, gegen die Datenschutzkontrolle Lobbypolitik zu betreiben, an allererster Stelle die Anwaltsverbände und -kammern. Obwohl es weiterhin praktisch keine Anwendungsfälle für einen Konflikt zwischen anwaltlicher Schweigepflicht bzw. Mandantengeheimnis und Datenschutzkontrolle gab, enthielt schon der erste Referentententwurf für eine Umsetzung der DSGVO eine sehr weitgehende Privilegierung. Diese wurde zwar modifiziert, aber im Wesentlichen bis zum Kabinettsentwurf vom 01.02.2017 fortgeschrieben. Dies stieß auf die einvernehmliche Kritik aller Datenschützer in Aufsichtsbehörden wie auch in Datenschutzorganisationen.

Bei der **Anhörung des Bundestags-Innenausschusses** am 27.03.2017 wurde die geplante Regelung von Peter Schaar von der EAID kritisiert: „Datenschutzbehörden müssen zukünftig draußenbleiben". Außer den Stellungnahmen der EAID und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) äußerten sich alle anderen dem Bundestag vorgelegten Stellungnahmen zum Thema entweder gar nicht oder kommentierten den Vorschlag positiv, so etwa die des Rechtsanwalts Piltz, der Wirtschaftsprüfer, des Arbeitgeberverbands BDA oder der Deutschen Krankenhausgesellschaft. Der Bundestag sah keine Veranlassung, insofern eine Änderung vorzunehmen.

2.2 Der Wortlaut

Folgende Regelung wurde beschlossen: *Gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuches genannten Personen oder deren Auftragsverar-*

beitern bestehen die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht im Sinne des Satzes 1 unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.

2.3 Die Begründung

Als Gesetzesbegründung wurde Folgendes ausgeführt: „Absatz 3 Satz 1 macht von der Öffnungsklausel des Artikels 90 der Verordnung (EU) 2016/679 Gebrauch, ihr entspricht Erwägungsgrund 164 der Verordnung. Nach Artikel 58 Absatz 1 Buchstaben e und f der Verordnung (EU) 2016/679 haben die Aufsichtsbehörden die Befugnis, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu erhalten zu allen für die Erfüllung ihrer Aufgaben notwendigen personenbezogenen Daten und Informationen sowie zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte. Artikel 90 Absatz 1 Verordnung (EU) 2016/679 eröffnet den Mitgliedstaaten die Möglichkeit, die Befugnisse der Aufsichtsbehörden im Sinne des Artikels 58 Absatz 1 Buchstaben e und f gegenüber Geheimnisträgern zu regeln. Mit Absatz 3 Satz 1 wird diese Möglichkeit insbesondere dergestalt umgesetzt, dass eine Aufsichtsbehörde entgegen Artikel 58 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 dann keinen Zugang zu Daten und Informationen hat, soweit dadurch die Geheimhaltungspflicht verletzt würde. Ohne eine Einschränkung der Befugnisse der Aufsichtsbehörden käme es zu einer Kollision mit Pflichten des Geheimnisträgers. Gerade bei den freien Berufen schützt die berufsrechtliche Schweigepflicht das Vertrauen des Mandanten und der Öffentlichkeit in den Berufsstand. Nach bundesverfassungsgerichtlicher Rechtsprechung darf das Mandatsverhältnis nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet sein (vgl. BVerfG, Urteil vom 12. April 2005 – 2 BvR 1027/02). Absatz 3 Satz 2 verlängert die Geheimhaltungspflicht auf die Aufsichtsbehörde. Berufsgeheimnisträger bedienen sich vermehrt externer IT-Dienstleister und verpflichten diese als Auftragsverarbeiter vertraglich zur Verschwiegenheit. Um zu vermeiden, dass die Auftragsverarbeiter vertragsbrüchig werden, wenn sie die ihnen anvertrauten Daten gegenüber den Aufsichtsbehörden offenlegen müssten, umfasst Absatz 3 auch den Auftragsverarbeiter.“

3 Auslegungsversuche des § 29 Abs. 3 BDSG

Absatz 3 privilegiert die in § 203 Abs. 1, 2a u. 3 StGB genannten **berufsausübende Personen**. Dabei handelt es sich nicht nur um den Arzt und den Rechtsanwalt, sondern auch um Zahnärzte, Apotheker, Angehörige eines anderen Heilberufs, Berufspsychologen, Patentanwälte, Notare, weitere Verteidiger, Wirtschaftsprüfer, vereidigte Buchprüfer, Steuerberater, Steuerbevollmächtigte, Mitglieder eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- und Steuerberatungsgesellschaft, Ehe-, Familien-, Erziehungs- und Jugendberater, Berater für Suchtfragen und für Schwangerschaftskonflikte, staatliche anerkannte Sozialarbeiter oder Sozialpädagogen, Angehörige einer privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle, Beauftragte für den Datenschutz, Mitglieder einer Rechtsanwaltskammer sowie um berufstätig tätige Gehilfen und die Personen, die bei Berufsgeheimnisträgern zur Vorbereitung auf den Beruf tätig sind. Sämtliche der genannten Personen bzw. Berufsgruppen setzen in zunehmendem Maße elektronische Datenverarbeitung ein und nutzen offene Kommunikationsnetze bei der Verarbeitung sensitiver personenbezogener Daten.

Neu ist, dass nicht nur die Verantwortlichen selbst und die bei diesen tätigen Personen privilegiert werden, sondern auch deren **Auftragsverarbeiter**. Diese genießen bisher noch nicht den Schutz des Berufsgeheimnisses. Dies soll sich aber noch vor Ablauf der Legislaturperiode im Herbst 2017 ändern. In einem vom Bundeskabinett am 15.02.2017 beschlossenen „Entwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ werden Personen ähnlich Berufsgeheimnisträgern unter einen rechtlichen Schutz gestellt, die bei Berufsgeheimnisträgern „an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist“. Diese aus Datenschutzsicht sehr zu begrüßende Regelungsabsicht bezieht sich auf für die Berufsausübung erforderliche Auftragsverarbeitungen für Berufsgeheimnisträger und nicht nur auf Auftragsverarbeitungen mit Berufsgeheimnissen.

Ausgeschlossen werden die in Art. 58 Abs. 1 lit. e u. f DSGVO geregelten Befugnisse der Aufsichtsbehörden. Dies sind der **„Zugang zu allen personenbezogenen Daten und Informationen“** sowie der „Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte“. Ausgeschlossen wird also nicht nur die Nutzung der Berufsgeheimnisse für datenschutzrechtliche Kontrollzwecke, sondern schon der Zugang zu diesen und damit auch die Prüfung, ob es sich dabei überhaupt um Berufsgeheimnisse handelt.

Die Kontrollprivilegierung des Abs. 3 besteht nur, „soweit die Inanspruchnahme der Befugnisse zu einem **Verstoß gegen die Geheimhaltungspflichten** dieser Personen führen würde“. Diese Beschränkung der Privilegierung macht ratlos: Eine Durchbrechung von Geheimhaltungspflichten liegt in jeder Form der Offenbarung. Ein Verstoß liegt dabei nicht vor, wenn die Offenbarung gerechtfertigt ist. Die Regelung gibt für eine solche Rechtfertigung keine Hinweise.

Eine Rechtfertigung kann in einer wirksamen **Einwilligung**, einer **Schweigepflichtentbindung** des Betroffenen, also z. B. des Mandanten oder des Patienten, liegen. Eine solche bezieht sich aber nur auf die diesen selbst betreffenden Daten. Regelmäßig erfassen die Datensätze aber nicht nur Angaben über einen Betroffenen, sondern auch zu weiteren Personen, die z. B. über eine Kontrollbitte bei einer Datenschutzaufsichts-

behörde keine „Einwilligung“ erteilt haben. Dies gilt erst recht, wenn, was bei Berufsgeheimnisträgern und deren Auftragsverarbeitern üblich ist, die Speicherung von Daten nicht (ausschließlich) nach individuellem Personenbezug getrennt, sondern in nicht abgeschotteten Datenbeständen erfolgt. Eine Einwilligung einer betroffenen Person genügt hier in keinem Fall, da andere Personen betroffen sind, die keine Einwilligung erteilt haben. Der Zugang zu deren Daten wird durch Abs. 3 ausgeschlossen und damit oft auch zwangsläufig der Zugang zu den Daten eines Einwilligenden (z. B. des Beschwerdeführers).

Jenseits von Einwilligungen können Offenbarungen nach § 203 StGB durch eine Interessenabwägung auf gesetzlicher Grundlage gerechtfertigt sein. Die einzige hier in Betracht kommende Rechtfertigung ist die Datenschutzkontrolle. Diese wird durch die Regelung aber gerade eingeschränkt. Wir haben es also bei § 29 Abs. 3 BDSG mit einer typischen **Zirkelverweisung**, also mit einer Verweisung auf sich selbst zu tun: Eine Datenschutzkontrolle nach Art. 58 DSGVO könnte die Offenbarung nach § 203 StGB rechtfertigen; mit ihr wäre aber in jedem Fall ein Verstoß gegen die Geheimhaltungspflichten des Geheimnisträgers verbunden. Die Regelung ist unklar und gibt weder dem Kontrollierten noch den Kontrollierenden Vorgaben, wann ein Verstoß gegen Geheimhaltungspflichten gegeben ist.

In der **Gesetzesbegründung** wird ausschließlich auf das Mandantengeheimnis Bezug genommen. Eine Beschränkung der Anwendung auf diesen Bereich wird aber durch den weiten und offenen Gesetzeswortlaut, der sogar Auftragsverarbeiter einbezieht, ausgeschlossen. Auch der Verweis der Gesetzesbegründung auf den Beschluss des Bundesverfassungsgerichts (BVerfG) vom 12.04.2005 gibt keine weiteren Hinweise auf eine mögliche Auslegung der Regelung. Dieser Beschluss schließt nicht den reinen Datenzugriff aus, sondern die umfassende staatsanwaltschaftliche Sicherstellung und Beschlagnahme. Er bezieht sich auf einen Rechtsanwalt und Steuerberater und nicht auf sämtliche Berufsgeheimnisträger oder auf solche Geheimnisträger generell (s. u. 4).

4 Die Datenschutzkontrolle aus verfassungsrechtlicher Sicht

Die Datenschutzkontrolle ist in **Art. 8 Abs. 3 Europäische Grundrechte-Charta** (GRCh) ausdrücklich vorgesehen: „Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht“. Eine Einschränkung hinsichtlich Berufsgeheimnisse enthält die Regelung nicht. Art. 8 Abs. 3 GRCh fordert ein effektives Datenschutzkontrollsystem, unabhängig davon, ob Berufsgeheimnisse verarbeitet werden oder nicht. Hierfür ist es nötig, dass die Kontrollstellen Untersuchungsbefugnisse erhalten, die sie jederzeit, d. h. nicht nur bei Vorliegen eines konkreten Verdachts und bezügliche jedweder Form der Verarbeitung benötigen.

Das Untersuchungsrecht der Kontrollstellen setzt nicht einmal eine personenbezogene Datenverarbeitung voraus; es genügt der **konkrete Verdacht** einer solchen Verarbeitung aufgrund tatsächlicher Anhaltspunkte. Nur wenn erkennbar ist, dass keine personenbezogene Datenverarbeitung erfolgt, besteht keine Auskunftspflicht und kein Kontrollrecht. Für die Überprüfung bedarf es grds. keines konkreten Anlasses, z. B. eines Verdachts eines Datenschutzverstoßes.

Auch nach **nationalem Verfassungsrecht** ist eine wirksame aufsichtliche Kontrolle zwingend. Zwar bedarf es hierfür generell nicht, wie im sicherheitsbehördlichen Bereich, turnusgemäßer Pflichtkontrollen. Wohl aber müssen situative aufsichtliche Kontrollen uneingeschränkt möglich sein. Es darf keinen kontrollfreien Raum geben. Die Daten müssen der Datenschutzkontrolle in praktikabel auswertbarer Weise zur Verfügung stehen.

Gerade bei tief in die Privatsphäre eingreifenden Maßnahmen der Datenverarbeitung ist eine aufsichtliche Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis von großer Bedeutung. Die Verarbeitung von Berufsgeheimnissen ist eine derart einschneidende bzw. sensitive Maßnahme.

Zweifellos erfolgen über Datenschutzkontrollen bei Berufsgeheimnisträgern, ähnlich wie über strafprozessuale Ermittlungsmaßnahmen, **Eingriffe in die Grundrechte** sowohl des Berufsgeheimnisträgers wie auch der von der Verarbeitung betroffenen Person, insbesondere in den Schutzbereich des Art. 2 Abs. 1 GG (Art. 6 GRCh) und in das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (Art. 8 GRCh). Auch das Grundrecht der Berufsfreiheit (Art. 12 GG, Art. 15 GRCh) ist bei der Datenschutzprüfung zu beachten. Bei Eingriffen ist die berufliche Sphäre von Rechtsanwälten oder von Steuerberatern und damit zudem die objektive Bedeutung der „freien Advokatur“ bzw. die Organstellung in der Steuerrechtspflege zu berücksichtigen. Dies darf aber nicht zu einer vollständigen Verhinderung der datenschutzrechtlichen Kontrolle führen. Vielmehr muss eine Prüfung der Verhältnismäßigkeit erfolgen.

Als Eingriffsgrundlagen sind allgemeine **gesetzliche Regelungen**, die eine staatliche Kontrolle erlauben, zulässig. Eine nähere gesetzliche Eingrenzung ist wegen der Vielgestaltigkeit möglicher Sachverhalte oft nicht möglich und auch verfassungsrechtlich nicht geboten. Die Befugnisse der Art. 58 Abs. 1 lit. e, f DSGVO genügen diesen verfassungsrechtlichen Anforderungen an hoheitliche Ermittlungsmaßnahmen. In Bezug auf den Schutz von Berufsgeheimnisträgern ist in jedem Fall eine Abwägung im Einzelfall erforderlich.

In diesen Bereichen muss eine „strenge **Begrenzung auf die Ermittlungszwecke**“ erfolgen. Zwar dürfen die im Rahmen einer Ermittlung erlangten Informationen zur Kenntnis genommen werden. Doch dürfen die überschießenden, für die Datenschutzkontrolle nicht erforderlichen Daten nicht weiterverarbeitet werden. Soweit eine Trennung möglich ist, ist diese vorzunehmen. Relevant können gerade bei der datenschutzrechtlichen Bewertung die Struktur des Datenbestands und die technisch-organisatorischen Rahmenbedingungen der Verarbeitung sein. Dies setzt aber eine Durchsicht der vorhandenen Daten voraus. Der jeweilige Eingriff im Rahmen der Kontrolle kann dabei von der Bedeutung der Kontrolle für den Schutz informationeller Selbstbestimmung und der Schwere eines aufzuklärenden Verstoßes abhängig gemacht werden.

Die verfassungsrechtlichen Bewertungen auf **nationaler und auf euro-**

päischer Ebene entsprechen sich vollständig. Art. 90 DSGVO erlaubt keinen gänzlichen Ausschluss der Untersuchungsbefugnisse in konkreten Situationen.

5. Verfassungswidrigkeit von § 29 Abs. 3 S. 1 BDSG

Angesichts dessen hält § 29 Abs. 3 BDSG einer verfassungsrechtlichen Prüfung nicht stand. Dadurch, dass gemäß der Regelung der Datenschutzkontrolle schon der Zugang zu Räumlichkeiten und Datenbeständen vorenthalten werden kann, wird für sie unter Umständen von vornherein eine **Kontrolle vollständig ausgeschlossen**. Ein Verantwortlicher oder Auftragsverarbeiter kann eine Kontrolle verweigern, ohne dass es der Datenschutzaufsicht ermöglicht wird, diese auf ihre Berechtigung hin zu überprüfen, da für eine solche Prüfung zumindest eine äußere Sichtung der zu kontrollierenden Datenbestände nötig ist. Es ist der Datenschutzaufsicht nicht zumutbar, bei jedem Konfliktfall eine gerichtliche Klärung herbeizuführen. Bis zur gerichtlichen Klärung könnten prüfrelevante Änderungen durch den Verantwortlichen oder Auftragsverarbeiter vorgenommen und damit Nachweise für Datenschutzverstöße beseitigt werden. Datenschutzverstöße im besonders sensitiven Geheimnisbereich bleiben unaufgeklärt und ohne Sanktion. Dies hätte zur Folge, dass gerade in einem Bereich, in dem die Beachtung des Datenschutzes von größter Bedeutung ist, ein noch stärkeres Vollzugsdefizit als bisher entstünde. Es wäre auch nicht im Sinne des Grundrechtsschutzes, bei Feststellung von Datenschutzverstößen durch die Aufsichtsbehörde die Weitergabe der relevanten Informationen an die Strafverfolgung auszuschließen.

Die **Unbestimmtheit der Regelung** provoziert geradezu Kontroversen über die Kontrollbefugnis. Angesichts der begrenzten Ressourcen der Datenschutzkontrolle kann die Unbestimmtheit der Regelung dazu führen, dass wirksame Prüfungen im Geheimnisbereich unmöglich würden.

Dies hätte zur Folge, dass eine effektive Prüfung der Verarbeitung personenbezogener Daten bei den in § 203 StGB genannten Personen bzw. Stellen verhindert würde. Eine Prüfung würde gerade dort eingeschränkt, wo wegen des Umfangs und der Sensibilität der Daten eine besondere Gefährdung für den Datenschutz bzw. für das Recht auf informationelle Selbstbestimmung besteht, also in Krankenhäusern, ambulanten Arztpraxen, bei privaten Versicherungen, Steuerberatern oder sozialen Beratungsstellen.

§ 29 Abs. 3 BDSG unterstellt fälschlich, dass es eine strukturell angelegte Konfliktlage zwischen dem Berufsgeheimnissen und dem Datenschutz gäbe. Die Regelung gibt im Konfliktfall den Berufsgeheimnissen vor dem Datenschutz den Vorrang. **Berufsgeheimnisse sind spezifische Datenschutzregelungen**, deren Einhaltung zu prüfen insbesondere Aufgabe der Aufsichtsbehörden ist. Andere hoheitliche Kontrollstellen, etwa die Staatsanwaltschaften oder die Berufskammern, sind – aus unterschiedlichen Gründen – für eine wirksame umfassende Kontrolle nicht geeignet.

Berufsgeheimnisse und berufliche Vertrauensverhältnisse bestehen vorrangig im Interesse der betroffenen Kunden, Mandanten oder Patienten und erst in zweiter Linie im Interesse der Geheimnisträger und schon gar nicht in deren Interesse an einer kontrollfreien Tätigkeit. Das Vertrauensverhältnis zwischen Geheimnisträger und den betroffenen Menschen würde eher dadurch beeinträchtigt, dass die Betroffenen befürchten müssten, dass ihre Geheimnisse bei den Berufsgeheimnisträgern mangels hinreichender Kontrolle nicht ausreichend geschützt sind.

Die Regelung des § 29 Abs. 3 BDSG lässt sich auch nicht mit der **Öffnungsklausel** des Art. 90 DSGVO in Einklang bringen. Diese erlaubt eine Einschränkung der Befugnisse der Aufsichtsbehörden nur, soweit dies „notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen“. Die obigen Ausführungen haben gezeigt, dass weder die Geeignetheit noch die Angemessenheit für diesen Zweck bestehen.

Als **vertretbare und hinreichende Schutzmaßnahme** i. S. v. Art. 90 DSGVO zugunsten des Berufsgeheimnisses genügt eine Regelung, die der Intention von § 29 Abs. 3 S. 2 BDSG entspricht, wonach die Aufsichtsbehörde selbst einer Geheimhaltungspflicht unterworfen wird. Auch in Bezug auf den Prüfanlass sind bei Berufsgeheimnissen gesetzliche Einschränkungen vorstellbar, etwa dass der Anlass für die Kontrollen näher definiert wird oder dass der Umfang von anlasslosen Kontrollen auf Stichprobenprüfungen beschränkt wird.

Im Ergebnis kann festgehalten werden, dass § 29 Abs. 3 BDSG gegen das grundrechtlich begründete **staatliche Gebot des Schutzes personenbezogener Daten** verstößt und deshalb aufgehoben werden muss. Sollten Berufsgeheimnisträger unter Verweis auf diese Regelung eine Datenschutzkontrolle verweigern, so ist die Datenschutzaufsichtsbehörde gut beraten, die Kontrolle mit den bestehenden aufsichtlichen Mitteln dennoch durchzusetzen und eine höchstgerichtliche Klärung der Verfassungskonformität der Regelung frühestmöglich anzustreben.


Bild: ClipDealer

Werner Hülsmann

Beschäftigtendatenschutz nach der DS-GVO und dem BDSG-neu

Neue Herausforderungen – auch für Betriebs- und Personalräte

Einleitung

Die mit der EU-Datenschutzgrundverordnung (DS-GVO) einher gegangene Reformierung des Datenschutzrechts auf europäischer und auf nationaler Ebene hätte die Chance geboten EU-weit einheitliche Rahmenbedingungen für den Beschäftigtendatenschutz zu schaffen. Diese Chance wurde leider vertan. So bleibt es Aufgabe der nationalen Gesetzgeber sowie der Arbeitgeber gemeinsam mit den Interessenvertretungen der Beschäftigten rechtliche Regelungen zum Beschäftigtendatenschutz zu schaffen.

Beschäftigtendatenschutz in der DS-GVO

Die DS-GVO regelt den Beschäftigtendatenschutz selbst nicht, sondern gibt mit einer sogenannten Öffnungsklausel in Artikel 88 Abs. 1 DS-GVO die Möglichkeit über nationales Recht und/oder Kollektivvereinbarungen – zu denen in Deutschland neben Tarifverträgen auch Betriebs- und Dienstvereinbarungen gehören – Regelungen zum Beschäftigtendatenschutz zu schaffen. Damit haben der nationale Gesetzgeber aber auch Arbeitgeber und die Interessenvertretungen der Beschäftigten die Möglichkeit den Beschäftigtendatenschutz zu regeln und insbesondere im Bereich der Dienst- und Betriebsvereinbarungen bewährte Regelungen weitgehend beizubehalten.

In Artikel 88 Absatz 2 DS-GVO werden Mindestanforderungen aufgeführt, denen derartige nationale Regelungen und Kollektivvereinbarungen zu genügen haben:

„Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.“

Es ist davon auszugehen, dass in vielen der bestehenden Betriebs- und Dienstvereinbarungen die geforderten „angemessenen und besonderen Maßnahmen“ noch nicht oder nicht in ausreichender Form enthalten sind.

Beschäftigtendatenschutz im neuen Bundesdatenschutzgesetz

Der Bundesgesetzgeber hat mit dem „Datenschutz-Anpassungs- und Umsetzungsgesetz EU“ (DSAnpUG-EU) in Artikel 1 das am 25. Mai 2018 in Kraft tretende neue Bundesdatenschutzgesetz (BDSG-neu)[1] beschlossen. Er hat es dabei allerdings wieder einmal versäumt ein Beschäftigtendatenschutzgesetz zu erlassen, obwohl ein solches schon lange gefordert wird und auch mehrfach in Koalitionsvereinbarungen versprochen wurde. Vielmehr hat sich der Bundesgesetzgeber damit begnügt im § 26 des BDSG-neu die Regelungen des § 32 des derzeitigen BDSG zu übernehmen und – um zu versuchen, die Anforderungen der DS-GVO zu erfüllen – etwas ergänzt. Allerdings gibt es berechtigte Zweifel, ob die Regelungen des § 26 BDSG-neu den Anforderungen des Art. 88 Abs. 2 DS-GVO genügen.

Begriffsbestimmung Beschäftigte

Die Definition des Begriffes „Beschäftigte“ findet sich in § 26 Abs. 8 BDSG-neu und nicht – wie eigentlich zu vermuten gewesen wäre – in § 2 BDSG-neu. Ist dies vielleicht ein Indiz dafür, dass zumindest langfristig beabsichtigt ist, den Beschäftigtendatenschutz doch noch – mitsamt der hierfür erforderlichen Begriffsbestimmung – in einem eigenständigen Gesetz zu regeln?

Diese Begriffsbestimmung übernimmt weitgehend die Begriffsbestimmung aus dem derzeitigen § 3 Abs. 11 BDSG-alt. Ergänzt wird sie um „Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher“ sowie um „Freiwillige, die einen Dienst nach dem (…) dem Bundesfreiwilligendienstgesetz leisten“.

Datenverarbeitung zum Zwecke des Beschäftigungsverhältnisses

In § 26 Abs. 1 Satz 1 BDSG-neu wird zum einen der bisherige Satz 1 des § 32 Abs. 1 BDSG-alt übernommen. Zum anderen wird ausdrücklich angegeben, dass eine Verarbeitung von Beschäftigtendaten auch zulässig ist, soweit diese zur „Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten“ erforderlich ist.

§ 26 Abs. 1 Satz 2 BDSG-neu übernimmt inhaltsgleich die Regelung aus § 32 Abs. 1 Satz 2 BDSG-alt zur Verarbeitung von Beschäftigtendaten zum Zweck der Aufdeckung von im Beschäftigungsverhältnis begangen Straftaten. Jedoch wurden die Begrifflichkeiten an die DS-GVO angepasst.

Die Abs. 6 und 7 des § 26 BDSG-neu übernehmen die Regelungen der Abs. 2 und 3 des derzeitigen § 32, wenn auch in umgekehrter Reihenfolge und mit sprachlichen Anpassungen. So sagt § 26 Abs. 6 BDSG lapidar: „Beteiligungsrechte der Interessenvertretungen der

Beschäftigten bleiben unberührt". Abs. 7 regelt nun, dass die Abs. 1 bis 6 auch dann gelten,

„wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen"

Einwilligung im Beschäftigungsverhältnis

Für Einwilligungen im Beschäftigungsverhältnis gibt § 26 Abs. 2 BDSG-neu Hilfestellung zur Beurteilung der Freiwilligkeit dieser Einwilligungen:

„(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 [das ist die DS-GVO] in Textform aufzuklären"

Diese Regelungen ergänzen und konkretisieren insoweit die allgemeinen Regelungen zur Einwilligung des Art. 7 DS-GVO.

Verarbeitung besonderer Kategorien personenbezogener Daten

Während das derzeitige BDSG keine besonderen Regelungen zur Verarbeitung von besonderen Kategorien personenbezogener Daten im Beschäftigungsverhältnis enthält, regelt nun § 26 Abs. 3 BDSG-neu den Umgang mit diesen besonders sensiblen Daten. Danach ist die Verarbeitung dieser Daten

„für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt".

Eine Einwilligung kann für die Verarbeitung besonderer Kategorien personenbezogener Daten erteilt werden, in diesem Fall muss sich die Einwilligung ausdrücklich auf diese besonderen Kategorien beziehen.

Der Arbeitgeber ist verpflichtet bei der Verarbeitung besonderer Kategorien personenbezogener Daten „angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person" zu ergreifen. Hierzu sind 10 Punkte in § 22 Abs. 2 BDSG-neu aufgeführt worden. Auf deren Darstellung wird an dieser Stelle verzichtet.

Kollektivvereinbarungen als Rechtsgrundlage

Im Absatz 4 des § 26 BDSG-neu ist ausdrücklich geregelt, dass eine Verarbeitung von Beschäftigtendaten, einschließlich besonderer Kategorien personenbezogener Daten auch auf Grundlage einer Kollektivvereinbarung zulässig ist. Hierbei wird zusätzlich darauf hingewiesen, dass die Regelungen des Art. 88 Abs. 2 DS-GVO bei derartigen Vereinbarungen einzuhalten sind.

Einhaltung der Grundsätze der DS-GVO

Absatz 5 des § 26 BDSG-neu fordert eine Selbstverständlichkeit:

„Der Verantwortliche muss geeignete Maßnahmen ergreifen um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 [das ist die DS-GVO] dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden".

Auch wenn das Bundesinnenministerium im Gegensatz zur EU-Kommission konsequent von Öffnungsklauseln in der DS-GVO spricht, sollte eigentlich klar sein, dass diese Konkretisierungs- und Ergänzungsklauseln nur im Rahmen der DS-GVO genutzt werden können.

Technischer Datenschutz – Ein Thema auch für Betriebs- und Personalräte?!

Auch wenn in den Anforderungen des Art. 88 Abs. 2 DS-GVO an Regelungen zum Beschäftigtendatenschutz nur der Begriff „Maßnahmen" genannt ist, sind damit auch die technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes gemeint. Zu den Anforderungen, die von der DS-GVO an den technischen Datenschutz und damit auch an diese technischen und organisatorischen Maßnahmen gestellt werden vgl. den Artikel „Technischer Datenschutz und Datenschutz-Folgenabschätzung – Anforderungen der DS-GVO" in dieser Ausgabe.

Für betriebliche und behördliche Datenschutzbeauftragte ist es selbstverständlich, dass sie sich mit dem Thema des technischen Datenschutzes beschäftigen (müssen). Aber es gehört – spätestens mit dem Gültigwerden der Regelung des Art. 88 Abs. 2 DS-GVO – auch zu den Aufgaben der Betriebs- und Personalräte darauf zu achten, dass der Arbeitgeber die erforderlichen „angemessenen und besonderen Maßnahmen" im Bereich der Verarbeitung von Beschäftigtendaten umgesetzt hat. Dies ergibt sich beispielsweise aus § 80 Abs. 1 BetrVG[2]:

„Der Betriebsrat hat folgende allgemeine Aufgaben:

1. darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden;"

Zu den „zugunsten der Arbeitnehmer geltenden Gesetze" gehören gemäß der höchstrichterlichen Rechtsprechung auch die entsprechenden gesetzlichen Regelungen zum Beschäftigtendatenschutz, damit neben § 26 des BDSG-neu auch Art. 88 DS-GVO.

Aufgaben für Betriebs- und Personalräte zum technischen Datenschutz

Für Betriebs- und Personalräte wird es in der Zukunft wichtig, sich intensiver mit dem technischen Datenschutz – also den technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes zu beschäftigen. Dies ergibt sich insbesondere aus zwei Gründen:

1. Aus der Regelung, dass bei einer gemäß Art. 35 DS-GVO durchzuführenden Datenschutz-Folgenabschätzung für eine Verarbeitung von Beschäftigtendaten der Arbeitgeber den Standpunkt der Personalvertretung einholen muss. Um eine qualifizierte Stellungnahme abzugeben, ist es für die Personalvertretung auch erforderlich einschätzen zu können, inwieweit die vom Arbeitgeber vorgesehenen technischen und organisatorischen Maßnahmen geeignet und ausreichend sind, um die mit dieser Verarbeitung verbundenen Risiken für die Beschäftigten zu minimieren.
2. Aus der Regelung, dass gemäß Art. 88 Abs. 2 DS-GVO Betriebs- und Dienstvereinbarungen, in denen der Umgang mit Beschäftigtendaten geregelt wird „angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person," umfassen müssen. Hier ist es die Aufgabe der Personalvertretungen bei Abschluss entsprechender Betriebs- oder Dienstvereinbarungen darauf zu achten, dass die seitens des Arbeitgebers vorgeschlagenen Maßnahmen zum einen ausreichend sind und zum anderen in der Betriebs- oder Dienstvereinbarung festgeschrieben werden. Letzteres kann aus praktischen Gründen auch in einer entsprechenden Anlage erfolgen, die fortgeschrieben werden kann, ohne dass hierzu eine Kündigung der Betriebs- oder Dienstvereinbarung erforderlich wäre.

Umgang mit bereits bestehenden Betriebs- und Dienstvereinbarungen.

Bereits bestehende Betriebs- und Dienstvereinbarungen sind zudem daraufhin zu überprüfen, ob sie den Anforderungen aus Art. 88 Absatz 2 DS-GVO genügen. Betriebs- und Dienstvereinbarungen, deren datenschutzrelevante Bestandteile diesen Anforderungen nicht genügen, sollten rechtzeitig angepasst werden. Alternativ kann auch eine Rahmen-Betriebs- oder Dienstvereinbarung geschlossen werden, die die im Art. 88 Abs. 2 DS-GVO geforderten Maßnahmen für bereits bestehende aber auch künftige Betriebs- und Dienstvereinbarungen enthält.

Falls die erforderliche Sachkunde bei den Personalvertretungen (noch) nicht vorhanden ist, sollte die Beratung durch den/die betrieblichen oder behördlichen Datenschutzbeauftragten und/oder die Hinzuziehung externen Sachverstandes erwogen werden.

Fazit

Auch wenn es noch immer kein Beschäftigtendatenschutzgesetz gibt, so führen die Neuregelungen in der DS-GVO und im BDSG-neu dazu, dass die bisher in den Betrieben geltenden Regelungen zum Beschäftigtendatenschutz – insbesondere die bereits bestehenden Betriebs- und Dienstvereinbarungen – auf den Prüfstand gestellt werden müssen. In vielen Fällen werden ergänzende Regelungen und Aktualisierung bestehender Regelungen erforderlich sein.

Vom Gesetzgeber ist nach wie vor zu fordern, dass er ein Beschäftigtendatenschutzgesetz erlässt, das diesen Namen auch verdient. An dieser Forderung wird sich der im Herbst neu zu wählende Bundestag und die neue Bundesregierung messen müssen. Das Netzwerk Datenschutzexpertise hat in einem Gutachten „Die EU-DSGVO und die Zukunft des Beschäftigtendatenschutzes" bereits im April 2016 entsprechende „Vorschläge für ein modernes Beschäftigten-/Arbeitnehmerdatenschutzrecht"[3] vorgestellt.

1 Für öffentliche Stellen der Länder ist zu beachten, dass hier die landesrechtlichen Regelungen zum Beschäftigtendatenschutz weiterhin gültig sind. Nur wo im Landesrecht geregelt ist, dass die entsprechenden Regelungen des BDSG anzuwenden sind, gilt auch für diese Stellen § 26 BDSG. Dies ist derzeit in sieben Bundesländern für öffentliche Stellen der Länder, die am Wettbewerb teilnehmen, so geregelt.

2 vergleichbare Regelungen finden sich auch in den Personalvertretungsgesetzen

3 Vgl. http://www.netzwerk-datenschutzexpertise.de/dokument/besch%C3%A4ftigtendatenschutz

Datenschutzwissen kompakt

Zusammenstellung: Werner Hülsmann

Band 4.1

Die Europäische Datenschutzgrundverordnung und das neue Bundesdatenschutzgesetz

Eine Synopse der Artikel und der Erwägungsgründe der EU-Datenschutzgrundverordnung (DSGVO) mit den entsprechenden Regelungen des ab dem 25. Mai 2018 geltendem neuen Bundesdatenschutzgesetz (BDSG-neu)



256 S., DIN A5-Querformat, Spiralbindung, ISBN 978-3-23456-041-9, 19,80 €

EfWeHa Verlag
Praxisbezogene Bücher für alle

In dieser neuen Synopse der ab 25. Mai 2018 gelten den EU-Datenschutzgrundverordnung (DS-GVO) sind zu den Artikeln der DS-GVO soweit wie möglich die passenden Erwägungsgründe der DS-GVO und die vergleichbaren Regelungen aus dem ebenfalls ab dem 25. Mai 2018 geltenden neuen Bundesdatenschutzgesetz (BDSG-neu) gegenübergestellt. Auch wurde für die DS-GVO ein (nicht-amtliches) Inhaltsverzeichnis hinzugefügt. Damit ist diese Synopse ein unverzichtbares Hilfsmittel für Datenschutzbeauftragte, DatenschutzjuristInnen, Datenschutzverantwortliche und alle am Datenschutz Interessierten.

https://efweha-verlag.de/bd41

Werner Hülsmann

Mobile Access unter den Bedingungen der EU-Datenschutz-Grundverordnung

1. Einleitung

Unter Mobile Access wird die Zutrittssteuerung mit mobilen Endgeräten, wie z.B. Mobiltelefon oder Smartphone verstanden. Bei der Zutrittssteuerung mit dem Smartphone fließen personenbezogene Daten und es gibt viele Beteiligte. Angefangen vom Nutzer des Smartphones über den Vertragsinhaber über den Mobilfunkbetreiber, weiter zum App-Ersteller und zu den Dienstleistern, die die entsprechenden Schließmechanismen anbieten und warten. Die Nutzung von Mobile-Access-Systemen bringt auf der einen Seite dem Anwender einen höheren Komfort. Auf der anderen Seite können aus den zwangsläufig entstehenden Daten von den unterschiedlichen Beteiligten mehr oder weniger lückenlose Bewegungsprofile erstellt werden. Für eine breite Akzeptanz derartiger Mobile-Access-Systeme ist daher ein datenschutzfreundlicher Umgang mit den anfallenden Daten zwingend erforderlich.

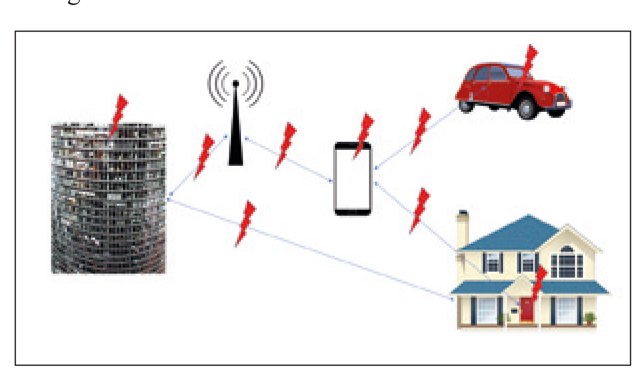


Bild 1: Datenflüsse und Angriffsmöglichkeiten

Gerade für die Anbieter derartiger Systeme und Dienstleistungen ist dabei zu beachten, dass ab dem 25. Mai 2018 die EU-Datenschutzgrundverordnung (DS-GVO) gültig wird. Sie bringt zum einen einige neue Anforderungen für Systembetreiber und Dienstleister und lässt zum anderen Datenschutzverstöße richtig teuer werden. Wesentliche Datenschutzgrundsätze der DS-GVO wie Datenminimierung und Datensparsamkeit gab es zwar bereits im bisherigen Bundesdatenschutzgesetz (BDSG). Neu ist aber, dass Verstöße gegen diese Grundsätze ab 25. Mai 2018 mit Bußgeldern in Millionenhöhe bedroht sind. Die DS-GVO eröffnet aber auch Chancen für die neuen Geschäftsmodelle. Unter anderem gibt es nun die Möglichkeit, dass mehrere Unternehmen vertraglich vereinbaren können, gemeinsam verantwortliche Stellen für die zu verarbeitenden personenbezogenen Daten zu sein. Dadurch ist es möglich, die Verantwortlichkeiten für den Umgang mit den personenbezogenen Daten zwischen den Beteiligten verbindlich zu regeln.

Mit Hilfe von Datenschutz-Zertifizierungen und der Anwendung von verbandsweiten Verhaltensregelungen kann die Einhaltung der Datenschutzgrundsätze dokumentiert werden. Dies kann dann auch zur Akzeptanzförderung genutzt werden.

2. Mobile Access und Datenschutz

Beim Mobile Access fallen an vielfältigen Stellen Daten an, Daten werden zwischen den Komponenten übertragen, werden von Systemanbieten gespeichert und verarbeitet. Daher stellt sich einige datenschutzrechtlich relevante Fragen.

- Welche der Daten sind personenbezogene Daten?
- Welche Daten sind „nur“ pseudonyme Daten, welche Daten können als anonymisierte Daten angesehen werden?
- Wer sind die Verantwortlichen (im bisherige Sprachgebrauch: Verantwortliche Stellen, also die Stellen, die die Daten der betroffenen Personen in eigener Verantwortung verarbeiten oder verarbeiten lassen)?
- Welche Anforderungen haben die verantwortlichen Stellen zu beachten?
- Welche Rechte haben die betroffenen Personen

2.1 Was sind personenbezogene Daten

Der Begriff „personenbezogene Daten“ wird in der DS-GVO in den Begriffsbestimmungen definiert. Diese Definition entspricht im Groben der Definition des derzeitigen Bundesdatenschutzgesetzes.

„Der Ausdruck […] ‘personenbezogene Daten‘ [bezeichnet] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind“ (Art. 4 Ziff. 1 DS-GVO)

Die Daten, die bei der Nutzung eines Mobile-Access-Systems durch die nutzende Person erzeugt werden und anfallen, sind daher grundsätzlich als personenbezogene Daten im Sinne der DS-GVO anzusehen. Hierzu gehören insbesondere (aber nicht nur) folgende Daten:

- Wer hat wann und wo welche Tür (Autotür, Wohnungstür, etc.) mit welchem Gerät bedient (geöffnet, verriegelt, …).
- Wer hat wann wo Licht, Heizung, etc. ein- oder ausgeschaltet.
- Wer hält sich wann wo auf.
- Wem ist welche SIM-Karte, welches Mobile Device zugeordnet.
- Wer hat wann wem welche Zugriffsrechte eingeräumt.
- Von wem wurden wann welche Zugriffsrechte genutzt.

Auch Daten, die z.B. zwischen einem Smartphone und der Türöffnungsmechanik eines KFZ hin und her fließen – sei es direkt (z.B. via Bluetooth oder NFC) oder indirekt über das Internet und einen Serviceprovider – sind personenbezogene Daten, da sowohl Smartphone als auch das KFZ einer Person zugeordnet werden können.

2.2 Wer ist „Herr der Daten", wer ist Verantwortlicher?

Gemäß Art 4 Ziffer 7 der DS-GVO bezeichnet der Ausdruck

> *„'Verantwortlicher' die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden" (Art. 4 Ziff. 7 DS-GVO)*

Von daher ist zur Klärung dieser Frage die Architektur des jeweilige Mobile-Access-Systems genauer zu betrachten. Dabei sind zwei unterschiedliche Grundkonstellationen möglich.

1. Es handelt sich um ein lokales System, d.h. die Datenübertragung zur Nutzung erfolgt – z.B durch Bluetooth, WLAN des Nutzers oder NFC – direkt zwischen dem Mobile Device und dem Schließsystem. In diesem Fall ist der Eigentümer bzw. Besitzer des Systems „Herr der Daten" und – im Falle eines z.B. im Unternehmen benutzten Schließsystems – Verantwortlicher im Sinne der DS-GVO.

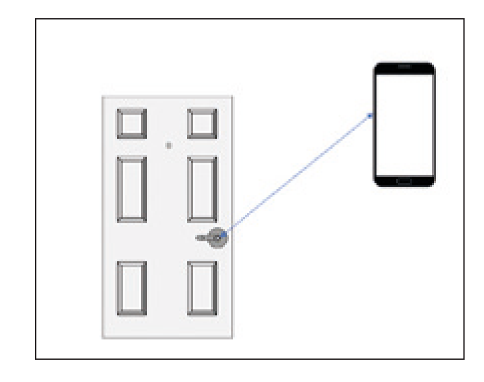


Bild 2: Lokales System

2. Es handelt sich um ein serverbasiertes System, das von einem Diensteanbieter betrieben wird. Die Daten, die zur Nutzung des Schließsystems verwendet werden, werden vom Mobile Device über das Internet zum Server und von diesem über das Internet zum Schließmechanismus übertragen. In diesem Fall ist der Diensteanbieter als Verantwortlicher im Sinne der DS-GVO anzusehen.

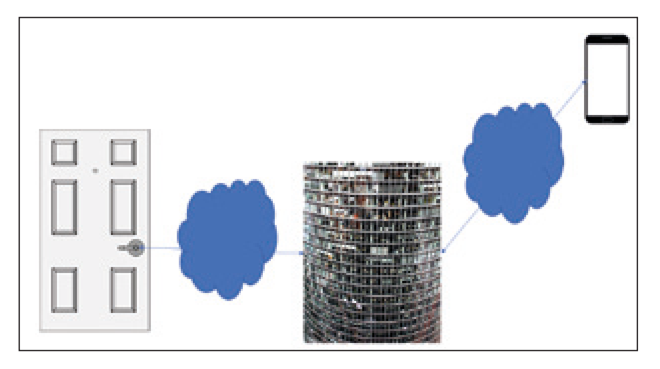


Bild 3: Serverbasiertes System

Bei diesen beiden Grundkonstellationen wird davon ausgegangen, dass

- sowohl der Mobilfunkbetreiber des Nutzers als auch die Internetprovider von Nutzer und Diensteanbieter hier als reine Telekommunikationsdienstleister agieren und die Daten, die zur Nutzung des Mobile-Access-Systems zwischen Mobile Device, Diensteanbieter und Schließsystem ausgetauscht werden, neutral übertragen und somit keine Mobile-Access-spezifischen Auswertungen oder Verarbeitungen vornehmen.
- die zur Nutzung des Mobile-Access-Systems für das Mobile Device erforderliche Software (Mobile-Access-App) vom Hersteller des Mobile Access-Systems oder in dessen Auftrag programmiert und zur Verfügung gestellt wird, die Mobile-Access-App also in den Verantwortungsbereich des Herstellers des Mobile-Access-Systems fällt.

Es ist allerdings auch denkbar, dass die genutzte Mobile-Access-Apps von unabhängigen Dritten erstellt und angeboten werden. Für Nutzer von Mobile-Access-Systemen könnten solche Apps dann interessant sein, wenn sie komfortabler sind als die herstellerseitig angebotenen oder wenn diese ermöglichen, auch solche Komponenten verschiedener Hersteller zu koppeln, bei denen das die Hersteller selbst nicht vorgesehen haben. Wenn über derartige Apps dann auch Nutzungsdaten gesammelt oder ausgewertet werden, sind diese Mobile-Access-App-Anbieter für die von ihnen gesammelten oder ausgewerteten Nutzungsdaten als Verantwortliche im Sinne der DS-GVO anzusehen.

2.3 Technischer Datenschutz in der DS-GVO

Die unterschiedlichen Systemkomponenten und Grundkonstellationen sind auch unter den Gesichtspunkten des technischen Datenschutzes zu betrachten.

Die DS-GVO stellt umfassende Anforderungen zur Sicherstellung der datenschutzkonformen Verarbeitung personenbezogener Daten. Hierzu sind von den Verantwortlichen „geeignete technische und organisatorische Maßnahmen" (Art. 24 Abs. 1 Satz 1 DS-GVO) umzusetzen. Diese Maßnahmen sollen insbesondere dazu dienen, die in der DS-GVO genannten Schutzziele zu erreichen. Zu den Schutzzielen und ihren Fundstellen siehe den Artikel „Technischer Datenschutz und Datenschutz-Folgenabschätzung – Anforderungen der DS-GVO" in dieser Ausgabe.

Einige mögliche Maßnahmen zur Erreichung der Schutzziele sind in der DS-GVO bereits genannt:

- Pseudonymisierung und Verschlüsselung (Art. 32, Abs. 1 Buchstabe a DS-GVO)
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32, Abs. 1 Buchstabe d DS-GVO)
- Verantwortliche und Auftraggeber müssen sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten (Art. 32, Abs. 4 DS-GVO)

Die weiteren erforderlichen Maßnahmen sind von den Verantwortlichen selbst festzulegen. Hierzu ist eine Risikoabschätzung und in vielen Fällen auch eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durchzuführen.

2.3.1 Anforderungen bei lokalen Systemen

Wird ein lokales System von einem privaten Nutzer ausschließlich für persönliche oder familiäre Zwecke genutzt, so unterliegt dieser privater Nutzer nicht der DS-GVO sondern ist vielmehr – wenn z.B. zu Wartungszwecken von einem Dienstleister Nutzungsdaten ausgelesen werden – als betroffene Person zu betrachten.

Wird dagegen ein lokales System im Unternehmen eingesetzt, so ist es in Bezug auf die Nutzungsdaten der Nutzer dieses Systems als Verantwortlicher anzusehen. Ein etwaiger Dienstleister, der das System im Auftrag des Unternehmens wartet oder administriert, wäre dann ein Auftragsverarbeiter im Sinne des Art. 28 DS-GVO, der die Daten nur auf Weisung des Verantwortlichen verarbeiten oder nutzen darf. In diesem Fall haben Verantwortlicher und Auftragsverarbeiter die datenschutzrechtlichen Anforderungen, die sich aus der Auftrags(daten)verarbeitung ergeben, zu berücksichtigen.

Die DS-GVO richtet sich nicht direkt an Hersteller von IT-Systemen. Aber Erwägungsgrund 78 der DS-GVO fordert:

„In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.“ (Erwägungsgrund 78, Satz 4, DS-GVO)

Wer die Hersteller hierzu wie ermutigen sollte, lässt die DS-GVO offen. Zumindest für Mobile-Access-Systeme, die (auch) im Unternehmensumfeld einsetzbar sein sollten, sollten sich die Hersteller diesen Satz zu Herzen nehmen. Schließlich stellt es einen teuren Bußgeldtatbestand dar, wenn ein einsetzendes Unternehmen die Prinzipien des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nicht nachweislich ausreichend berücksichtigt hat. Durch entsprechende Zertifizierungen, die die DS-GVO ausdrücklich vorsieht, können Hersteller den Unternehmen bei diesem Nachweis helfen. Auch den privaten Nutzern würden solche Zertifizierungen helfen, bei den Anbietern von Mobile-Access-Systemen die Spreu vom Weizen zu trennen.

Bei lokalen Systemen (vgl. Bild 2) sind in erster Linie drei Angriffsziele abzusichern:

1. Die App auf dem Mobile Device,
2. die Verbindung zwischen dem Mobile Device und dem Schließsystem und
3. das Schließsystem selbst.

Bei der Gestaltung der Mobile-Access-App ist zu berücksichtigen, dass das Mobile Device als unsicheres Gerät einzustufen ist. Die von den derzeitigen Standardbetriebssystemen angebotenen Sicherheitsfunktionen können nicht als ausreichend angesehen werden, wie die Veröffentlichung immer neuer Sicherheitslücken zeigt. Von daher ist es wichtig, dass in der App selbst weitergehende Schutzmechanismen eingebaut werden. So muss unter anderem sichergestellt sein, dass die App selbst mit einem PIN oder einem Passwort vor unbefugter Nutzung geschützt werden kann und dass die gespeicherten Daten wirksam verschlüsselt sind.

In Bezug auf die Verbindung zwischen dem Mobile Device und dem Schließsystem muss unter anderem sichergestellt werden, dass die Datenübertragung verschlüsselt erfolgt und dass sich sowohl das Mobil Device gegenüber dem Schließsystem als auch das Schließsystem sich gegenüber dem Mobile Devise durch Einsatz entsprechender kryptographischer Verfahren authentifiziert.

Das Schließsystem ist nicht nur – wie auch schon bisher – gegen physische Manipulationen zu schützen, sondern es ist auch gegen IT-technische Angriffe zu schützen. Dabei ist zu berücksichtigen, dass gerade bei Schließsystemen in abgelegenen oder unbeobachteten Objekten Brute-Force-Angriffe leicht möglich sind. Daher sind insbesondere aus anderen Zusammenhängen im Bereich der Authentifizierung bereits bekannte Verfahren einzusetzen. Hierzu gehört z.B. eine vorübergehende Sperre nach drei fehlerhaften Authentifizierungsversuchen, die nach jedem weiteren fehlerhaften Authentifizierungsversuch verlängert wird. Auch muss sichergestellt werden, dass ein abgehörter verschlüsselter Befehl zum Öffnen des Schließsystems nicht durch ein Aussenden einer Kopie dieses verschlüsselten Befehls zu einem späteren Zeitpunkt zum erneuten Öffnen des Schließsystems führt.

Bei der Auswahl der Verfahren ist soweit wie möglich sicherzustellen, dass ein erfolgreicher Angriff auf ein lokales Mobile-Access-System eines Herstellers nicht dazu führt, dass alle anderen Mobile-Access-Systeme der gleichen Baureihe ebenfalls geknackt sind. „Security by Obscurity“ sollte daher nicht zum Einsatz kommen. Denn Angreifer können derartige Systeme erwerben und dann ganz in Ruhe analysieren. Wirksame kryptographische Methoden, mit ausreichender Schlüssellänge und (automatischem) regelmäßigen Schlüsselwechsel sind da wesentlich zielführender.

2.3.2 Anforderungen bei serverbasierten Systemen

Bei serverbasierten Mobile-Access-Systemen (vgl. Bild 3), die von Herstel-

lern oder Dienstleistern betrieben werden, sind die Hersteller oder Betreiber der Systeme als Verantwortliche in der Pflicht, die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, die erforderlich sind, um die oben genannten Schutzziele zu erreichen.

Neben den im Abschnitt zu den lokalen Systemen (s.o., 2.4.1) genannten Anforderungen kommen für die Betreiber von serverbasierten Mobile-Access-Systemen weitere Anforderungen hinzu. Die Gewährleistung der Verbindungssicherheit ist komplexer, da mehr Komponenten als bei einem lokalen System beteiligt sind.

Der Betreiber des serverbasierten Mobile-Access-Systems wird selbst zu einem interessanten Angriffsziel und zwar zu einem deutlich interessanteren als ein einzelnes lokales Schließsystem. Ein Angreifer, der es schaffen sollte in die dortigen Server einzudringen, hätte – je nach Ausgestaltung des Systems – eventuell die Möglichkeit nicht nur ein Schließsystem zu öffnen, sondern viele verschiedene Schließsysteme an unterschiedlichen Orten. Von daher sind die Daten auf den Server – trotz ihres Schutzes durch Firewall und Intrusion Detection Systemen – so zu verschlüsseln, dass nur die befugten Personen sie nutzen können.

Eine Risiko- und eine Datenschutz-Folgenabschätzung wird für einen Betreiber eines serverbasierten Mobile-Access-Systems Pflicht sein. Auf dieser Grundlage sollte ein umfassendes Datenschutz- und IT-Sicherheitskonzept, dass alle oben genannten Schutzziele umfassend berücksichtigt und die entsprechenden Maßnahmen zur Risikovermeidung und -minimierung sowie zur Umsetzung des Datenschutzes vorsieht.

Ein ganz wichtiger Aspekt ist auch die Sicherstellung der Verfügbarkeit der serverbasierten Systeme und der entsprechenden Verbindungen.

Serverseitig ist sicherzustellen, dass eine nahezu 100%ige Verfügbarkeit sichergestellt wird. Alternativ müsste das Mobile-Access-System so gestaltet werden, dass zumindest eine Öffnung und Verriegelung der Schließsysteme über eine lokale Verbindung (z.B. Bluetooth, NFC) möglich ist.

Bezüglich der Datenverbindungen ist unter anderem zu überlegen, ob als Fallback zur Internetverbindung zumindest eine Öffnung und Verriegelung der Schließsysteme über eine SMS-basierte Lösung angeboten wird. Dies würde bedingen, dass ein im Haus oder Auto verbautes System auch über ein SIM-Karten-Modul verfügt, das bei Ausfall der Internetverbindung genutzt werden kann.

2.4 Rechte der betroffenen Personen

Es würde den Rahmen dieses Artikels sprengen, ausführlich und in aller Tiefe auf die Rechte der betroffenen Personen einzugehen. Es wird aber deutlich, dass die Umsetzung dieser Rechte bereits beim Entwurf und bei der Gestaltung der Mobile-Access-Systeme zu berücksichtigen sind.

Die wesentlichen sich aus der DS-GVO ergebenden Rechte der betroffenen Personen in Bezug auf Mobile-Access-Systeme sind:

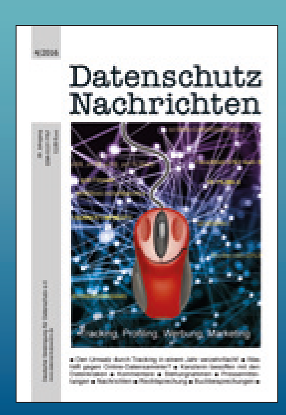
- Informationspflichten (Art. 13, 14 DS-GVO)
- Auskunftsrecht – Recht auf Kopie (Art. 15 DS-GVO)
- Recht auf Berichtigung (Art. 16 DS-GVO)
- Recht auf Löschung („Recht auf Vergessenwerden“) (Art. 17 DS-GVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)
- Mitteilungspflichten an Dritte über Berichtigung, Löschung und Einschränkung der Verarbeitung (Art. 19 DS-GVO)
- Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)
- Widerspruchsrecht (Art. 21 DS-GVO)
- Meldung von Datenschutzverletzungen (Art. 34 DS-GVO)

3 Fazit

Es liegt – schon aus Akzeptanzgründen – im Interesse der Hersteller und Anbieter von Mobile-Access-Systemen transparent über die vorgesehenen Verarbeitungen personenbezogener Daten zu informieren und standardmäßig nur die personenbezogenen Daten zu verarbeiten, die für den Betrieb der Systeme erforderlich sind. Falls Einwilligungen für weitergehende Verarbeitungen (z.B. für Komfortfunktionen) eingeholt werden sollen, müssen diese tatsächlich freiwillig sein und auf einfache Art und Weise widerrufen werden können.









online zu bestellen unter: **www.datenschutzverein.de/dana**

Werner Hülsmann

Technischer Datenschutz und Datenschutz-Folgenabschätzung in der DS-GVO

1 Einleitung

Eine der wesentlichen Änderungen, die sich durch die EU-Datenschutzgrundverordnung (DS-GVO) ergeben, ist die deutliche Ausweitung der Anforderungen an den technischen Datenschutz. Dies wird u.a. durch die Einführung der Datenschutz-Folgenabschätzung und durch ihre Ausgestaltung unterstrichen. Beide Aspekte sollen im Folgenden etwas ausführlicher dargestellt werden.

2 Technischer Datenschutz – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen – Sicherheit der Verarbeitung

2.1 Vergleichende Gegenüberstellung BDSG-alt, DS-GVO und BDSG-neu

BDSG-alt		DS-GVO (Art.) und BDSG-neu (§)			
§§	Inhalt	Art.	Abs.	Inhalt	ERW
§ 9	Anforderung technische und organisatorische Maßnahmen (TOM) zur Sicherstellung des Datenschutzes zu ergreifen	Art. 24	1 – 3[1]	Anforderung, TOM zur Sicherstellung DS-GVO-konformer Verarbeitung zu ergreifen	74 – 78
§ 3a	Datenvermeidung und Datensparsamkeit	Art. 25	1	Datenschutz durch Technikgestaltung	78
		Art. 25	2	Datenschutz durch datenschutzfreundliche Voreinstellung.	
		Art. 25	3	Genehmigtes Zertifizierungsverfahren als Nachweis der Anforderungen aus Abs. 1 und 2	
Anlage zu § 9	Schutzziele der TOM	Art. 25 Art. 32	1 1	Datenschutzgrundsätze des Art. 5 sind Schutzziele der TOM (Weitere) Schutzziele der TOM	83
		Art. 32	2	Risikoabschätzung	
		Art. 32	3	Verhaltensregeln und Zertifizierungsverfahren als Nachweis der Umsetzung	
§ 5	Verpflichtung auf das Datengeheimnis	Art. 32	4	Sicherstellung, dass Mitarbeiter Daten nur weisungsgebunden verarbeiten	
		§ 22	2	Maßnahmen bei der Verarbeitung besonderer Kategorien personenbezogener Daten	

2.2 Abweichung altes vs. neues Recht

Die meisten Anforderungen aus der DS-GVO an den technischen Datenschutz – nämlich Datenminimierung, Datenschutz durch Technikgestaltung und Umsetzung technischer und organisatorischer Maßnahmen – sind grundsätzlich bereits aus dem BDSG-alt bekannt. So fordert der § 3a BDSG-alt bereits „so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen“. Auch „die Auswahl und Gestaltung von Datenverarbeitungssystemen“ hat sich an diesem Ziel auszurichten. Die Anforderung an die verantwortliche Stelle und einen etwaigen Auftragnehmer, geeignete technische und organisatorische Maßnahmen zu treffen ist im § 9 BDSG-alt nebst Anlage zu § 9 vorhanden. Die Forderung des Art. 25 Abs. 2 – Datenschutz durch datenschutzfreundliche Voreinstellung – ist dagegen nicht ausdrücklich im BDSG-alt enthalten. Erwägungsgrund 78 der DS-GVO spricht davon, dass Hersteller von Produkten, Diensten und Anwendungen „ermutigt werden“ sollen, den Datenschutz bereits „bei der Entwicklung und Gestaltung ihrer Produkte, Dienste und Anwendungen zu berücksichtigen.“

Während Verstöße gegen die §§ 3a und 9 (nebst Anlage zu § 9) BDSG-alt für sich genommen bisher keinen Bußgeldtatbestand darstellen, sind Verstöße gegen die Art. 25 und 32 DS-GVO mit einem Bußgeld der Kategorie 10 Mio./2% bedroht. Verstöße gegen Art. 5 DS-GVO sind mit einem Bußgeld der Kategorie 20 Mio./4% bedroht.

Die Anforderung aus Art. 24 Abs. 2 DS-GVO an Verantwortliche erforderlichenfalls geeignete Datenschutzregelungen und –strategien einzuführen und umzusetzen, ist im BDSG-alt nicht ausdrücklich vorhanden. Gleichwohl wird in der Anlage zu § 9 Satz 1 BDSG-alt gefordert, dass „die innerbehördliche oder innerbetriebliche Organisation so zu gestalten [ist], dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.“ Dies impliziert auch die erforderlichen unternehmensinternen Datenschutzregularien.

Neu ist in der DS-GVO die ausdrückliche Erwähnung, dass genehmigte Verhaltensregeln und Zertifizierungsverfahren dem Nachweis der Umsetzung dieser Anforderungen dienen können.

Formal fällt zwar die Verpflichtung auf das Datengeheimnis aus § 5 BDSG-alt weg. Allerdings fordert Art. 32 Abs. 4 DS-GVO, dass der Verantwortliche und der Auftragsverarbeiter „Schritte unternehmen“, „um sicherzustellen, dass ihnen unterstellte natürliche Personen die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten“.

Die Formulierung und die Inhalte der Schutzziele hat sich gegenüber den bisherigen acht Schutzzielen der Anlage zu § 9 Abs. 1 BDSG-alt wesentlich geändert. Die Schutzziele technischer und

organisatorischer Maßnahmen verteilen sie auf mehrere Regelungen der DS-GVO. Diese sind im Folgenden zusammengefasst dargestellt.

Art. 25. Abs. 1 fordert die Umsetzung technischer und organisatorischer Maßnahmen zur Umsetzung der Datenschutzgrundsätze. Diese sind gemäß Art. 5 Abs. 1 DS-GVO:

a. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz,
b. Zweckbindung,
c. Datenminimierung,
d. Richtigkeit,
e. Speicherbegrenzung (Erforderlichkeitsgebot) und
f. Integrität und Vertraulichkeit.

Ergänzend fordert Art. 5 Abs. 2 DS-GVO die Einhaltung der Rechenschaftspflicht.

Art. 32 Abs. 1 DS-GVO wiederholt zum einen Schutzziele aus den Grundsätzen und nennt zum anderen weitere Schutzziele:

- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit beim Betrieb (Art. 32, Abs. 1 Buchst. b DS-GVO)
- Verfügbarkeit bei einem physischen oder technischen Zwischenfall (Art. 32, Abs. 1 Buchst. c DS-GVO)

Des Weiteren werden in Art. 32 DS-GVO auch konkrete Maßnahmen zur Erreichung dieser Schutzziele benannt:

- Pseudonymisierung und Verschlüsselung (Art. 32, Abs. 1 Buchst. a DS-GVO)
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32, Abs. 1 Buchst. d DS-GVO)
- Verantwortliche und Auftraggeber müssen sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten (Art. 32, Abs. 4 DS-GVO)

Zur Veranschaulichung sind nachfolgend die Schutzziele der DS-GVO aufgeführt:

Schutzziel	Fundstelle DS-GVO
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben	Art. 5, Abs. 1 Buchst. a
Transparenz	Art. 5, Abs. 1 Buchst. a, Art. 13 und Art. 14
Zweckbindung	Art. 5, Abs. 1 Buchst. b
Datenminimierung	Art. 5, Abs. 1 Buchst. c
Speicherbegrenzung (Erforderlichkeitsgebot)	Art. 5, Abs. 1 Buchst. e
Richtigkeit	Art. 5, Abs. 1 Buchst. d
Integrität	Art. 5, Abs. 1 Buchst. f, Art. 32, Abs. 1 Buchst. b
Vertraulichkeit	Art. 5, Abs. 1 Buchst. f, Art. 32, Abs. 1 Buchst. b
Verfügbarkeit und Belastbarkeit beim Betrieb	Art. 32, Abs. 1 Buchst. b
Verfügbarkeit bei einem physischen oder technischen Zwischenfall	Art. 32, Abs. 1 Buchst. c

2.3 Maßnahmen bei der Verarbeitung besonderer Kategorien personenbezogener Daten

§ 22 Abs. 2 des am 25. Mai 2018 in Kraft tretenden Bundesdatenschutzgesetz (BDSG-neu) verpflichtet Verantwortliche, die besondere Kategorien personenbezogener Daten verarbeiten, „angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person“ umzusetzen. Zu diesen Maßnahmen „können (..) insbesondere gehören:

1. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 [das ist die DS-GVO] erfolgt,
2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. Benennung einer oder eines Datenschutzbeauftragten,
5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
6. Pseudonymisierung personenbezogener Daten,
7. Verschlüsselung personenbezogener Daten,
8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
9. zur Gewährleitung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder
10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.“

Bei der Entscheidung über die Ergreifung der Maßnahmen sind

- der Stand der Technik,
- die Implementierungskosten und
- der Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie
- die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

zu berücksichtigen. Dies bedingt, das die getroffenen Maßnahmen in regelmäßigen Abständen zu überprüfen sind, da sich der Stand der Technik fortentwickelt und auch immer neue Angriffsmöglichkeiten entwickelt werden, was eine Neubewertung insbesondere der Eintrittswahrscheinlichkeit und der Schwere der Risiken erfordert.

2.4 Rechtliche Bewertung / Interpretation

Die Unternehmen haben bei der Verarbeitung personenbezogener Daten darauf zu achten, dass die Software und Syste-

me über datenschutzfreundliche Voreinstellungen verfügen. D.h. beispielsweise, dass Einwilligungen oder Zustimmungen – z.B. zur Lokalisierung – standardmäßig deaktiviert sein müssen und Nutzer und Nutzerinnen diese – wenn sie die entsprechenden Dienste nutzen wollen – ausdrücklich freigeben müssen.

Darüber hinaus sollten die Unternehmen auf Softwarehersteller und Dienstleister hinwirken, dass von diesen angebotene Software und Dienstleistungen datenschutzkonform entwickelt werden. Dies kann durch entsprechende Anforderungen bei der Ausschreibung oder der Angebotseinholung unterstützt werden.

Bezüglich der technischen und organisatorischen Maßnahmen reicht es künftig nicht mehr aus, die erforderlichen Maßnahmen zur Sicherstellung des Datenschutzes zu ergreifen. Vielmehr ist es künftig erforderlich die ergriffenen Maßnahmen zu dokumentieren und den Nachweis zu erbringen, dass sie regelmäßigen daraufhin überprüft werden, ob sie noch ausreichend sind und noch dem Stand der Technik entsprechen.

2.5 Handlungsbedarf

In Verbindung mit Art 5 Abs. 2 DS-GVO („Rechenschaftspflicht“) ist es – auch zur Vermeidung von Bußgeldrisiken – in den Unternehmen zwingend erforderlich, zum einen dafür zu sorgen, dass die erforderlichen technischen und organisatorischen Maßnahmen ergriffen werden und zum anderen dafür zu sorgen, dass diese Maßnahmen ausreichend dokumentiert werden um jederzeit nachweisen zu können, dass die getroffenen technischen und organisatorischen Maßnahmen ausreichend sind und dem aktuellen Stand der Technik entsprechen. Folgender konkreter Handlungsbedarf ist gegeben:

- Prüfen, ob in allen Anwendungen nur die Daten erhoben werden, die für die jeweiligen Zwecke erforderlich sind.
- Prüfen, ob in Eingabemasken und Formularen freiwillige Angaben deutlich als solche gekennzeichnet sind.
- Prüfen, ob in Eingabemasken Ankreuzfelder für Einwilligungen und Nutzungszustimmungen nicht vorangekreuzt sind.
- Prüfen, ob sichergestellt ist, dass Daten, die nur aufgrund einer Einwilligung verarbeitet werden dürfen, auch nur bei vorliegender wirksamer Einwilligung verarbeitet werden.
- Prüfung, ob die technischen und organisatorischen Maßnahmen – inklusive der entsprechenden Dienstanweisungen – dem aktuellen Stand der Technik entsprechen sowie unter Berücksichtigung der neu formulierten Schutzziele sowie der Risiken angemessen und ausreichend sind.
- Gegebenenfalls Anpassung der Maßnahmen.
- Prüfung und gegebenenfalls Aktualisierung der Dokumentation der technischen und organisatorischen Maßnahmen zum Datenschutz.
- Sicherstellen, dass eine regelmäßige Überprüfung dieser Maßnahmen erfolgt.
- Sollte bisher noch Datensicherheitskonzept erstellt worden sein, empfiehlt sich folgende Vorgehensweise:
  - Schutzbedarfsfeststellung, diese ist zu dokumentieren.
  - Risikobewertung, diese ist ebenfalls zu dokumentieren.
  - Festlegen, welche technischen und organisatorischen Maßnahmen erforderlich sind.
  - Umsetzung der Maßnahmen.
  - Dokumentation der erforderlichen und der getroffenen Maßnahmen.

3 Datenschutz-Folgenabschätzung

3.1 Vergleichende Gegenüberstellung BDSG-alt und DS-GVO

BDSG-alt			DS-GVO			
§§	Abs.	Inhalt	Art.	Abs.	Inhalt	ERW
4d	5	Pflicht zur Vorabkontrolle - Ausnahmen	35	1	Pflicht zu DS-Folgenabschätzung allgemein, zuständig: Verantwortlicher	84, 89, 90, 92
4d	6	Zuständig für die Vorabkontrolle: DSB		2	Verantwortlicher holt Rat des DSB ein	
				3	Pflicht zu DS-Folgenabschätzung, konkret Fälle	91 2
				4	Liste der Datenschutzaufsichtsbehörde von Verarbeitungstätigkeiten, bei denen eine Datenschutz-Folgeabschätzung erforderlich ist	
				5	Mögliche Liste der Datenschutzaufsichtsbehörde von Verarbeitungstätigkeiten, bei denen keine Datenschutz-Folgeabschätzung erforderlich ist	
				6	Kohärenzverfahren für die Listen nach Abs. 5 und 6	
				7	Inhalt der Datenschutz-Folgenabschätzung	
				8	Einhaltung genehmigter Verhaltensregeln sind zu berücksichtigen	
				9	Einholung des Standpunkts der betroffenen Personen oder ihrer Vertreter	
				10	Ausnahmen von den Abs. 1 bis 7	
				11	Überprüfung, ob Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird	

3.2 Abweichung altes vs. neues Recht

Die Regelung zur Datenschutz-Folgenabschätzung aus Art. 35 DS-GVO kann im weitesten Sinne als Nachfolgeregelung der Regelung zur Vorabkontrolle aus § 4d Abs. 5 und 6 BDSG-alt angesehen werden. Aus der bisher bekannten Vorabkontrolle wird quasi – vereinfacht ausgedrückt – die Datenschutz-Folgenabschätzung.

Ein wesentlicher Unterschied zwischen der künftigen Datenschutz-Folgenabschätzung und der bisherigen Vorabkontrolle ist der Umstand, dass nach dem bisherigen Recht der/die Datenschutzbeauftragte für die Vorabkontrolle zuständig ist und damit eine verbindliche Entscheidung über die datenschutzrechtliche Zulässigkeit eines Verfahrens zu treffen hat. Auch die Möglichkeit des Vorstandes oder der Geschäftsführung, sich über die Entscheidung des/der Datenschutzbeauftragten hinwegsetzen, ändert nichts an der Tatsache, dass nach dem bisherigen Recht der/die Datenschutzbeauftragte, dort wo eine Vorab-

kontrolle gesetzlich gefordert ist, die Entscheidung über die rechtliche Zulässigkeit einer Verarbeitung zu treffen und zu verantworten hat.

Die Datenschutz-Folgenabschätzung nach der DS-GVO ist demgegenüber von dem Verantwortlichen (im bisherigen Sprachgebrauch: von der verantwortlichen Stelle) durchzuführen. Der Verantwortliche hat nur noch den Rat des/der Datenschutzbeauftragten, sofern ein/e solche/r benannt wurde, einzuholen[3].

Ein weiterer wesentlicher Unterschied ist darin zu sehen, dass das bisherige BDSG-alt keinerlei Regelungen zur Ausgestaltung der Vorabkontrolle enthielt, während Art. 35 Abs. 7 DS-GVO regelt, dass die Datenschutz-Folgenabschätzung zumindest folgende Punkte enthalten muss:

a. „eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
b. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
c. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
d. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.“

Des Weiteren ist in Abs. 8 ausdrücklich geregelt, dass die „Einhaltung genehmigter Verhaltensregeln (…) bei der Beurteilung der Auswirkungen der (…) durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen“ ist.

Eine weitere wichtige Regelung findet sich in Art. 35 Abs. 9 DS-GVO: „Der Verantwortliche holt gegebenenfalls[4] den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.“

Daraus folgt, dass in der Regel bei der Einführung neuer IT-technischer Systeme, die eine Überwachung der Beschäftigten ermöglichen, der Verantwortliche – also der Arbeitgeber – bei der Durchführung der Datenschutz-Folgenabschätzung nicht nur den Rat des/der benannten Datenschutzbeauftragten einholen muss, sondern – unbeschadet der Mitbestimmungsrechte – auch den Standpunkt des Betriebs- oder Personalrates. Sofern es sich bei den betroffenen Personen um Verbraucher handelt, kommen hier auf die Verbraucherschutzverbände, aber auch auf Vereine, zu deren Themen u.a. der Datenschutz aus Verbrauchersicht gehört, neue Aufgaben und eine erhöhte Verantwortung zu.

Hinzugekommen ist die Verpflichtung der Datenschutz-Aufsichtsbehörden, eine Liste zu erstellen, die diejenigen Verarbeitungsvorgänge enthält, für die eine Datenschutz-Folgenabschätzung verpflichtend durchzuführen ist. Darüber hinaus kann die Datenschutz-Aufsichtsbehörde eine weitere Liste erstellen, die Arten von Verarbeitungsvorgängen enthält, für die keine Datenschutz-Folgenabschätzung erforderlich ist.

3.3 Rechtliche Bewertung / Interpretation

Nach derzeitigem Kenntnisstand (insbesondere Aufgrund von Aussagen von Vertreter/inne/n der Aufsichtsbehörden auf diversen Veranstaltungen) ist davon auszugehen, dass eine Datenschutz-Folgenabschätzung für Verarbeitungen, die bereits vor dem Stichtag 25. Mai 2018 begonnen wurden, aus Sicht der Aufsichtsbehörden dann nicht erforderlich ist, wenn für diese Verarbeitungen bereits eine Vorabkontrolle nach § 4d Abs. 5,6 BDSG-alt erfolgt ist und das Ergebnis derart dokumentiert wurde, dass das Ergebnis der Vorabkontrolle nachvollziehbar ist.

Während nach dem BDSG-alt die Nichtdurchführung einer erforderlichen Vorabkontrolle zur Unzulässigkeit dieses Verfahrens führte und damit die damit durchgeführten Verarbeitungen personenbezogener Daten als unzulässige Datenverarbeitungen bußgeldbewehrt waren, ist nach der DS-GVO bereits eine nicht durchgeführte aber erforderliche Datenschutz-Folgenabschätzung selbst ein Verstoß gegen die DS-GVO, der gemäß Art. 83 Abs. 4 DS-GVO mit einem Bußgeld in der Kategorie bis zu 10 Mio. € / 2 % vom Weltvorjahresumsatz geahndet werden kann. Hinzu kommt der mögliche Verstoß einer unzulässigen oder unzureichend abgesicherten Datenverarbeitung, der ergänzend mit einem Bußgeld in der Kategorie bis zu 20 Mio. € / 4% vom Weltvorjahresumsatz geahndet werden kann.

Darüber hinaus führt bei der Datenschutz-Aufsichtsbehörde die Nichtnachweisbarkeit der Entscheidung, ob für eine Verarbeitungstätigkeit eine Datenschutz-Folgenabschätzung vorzunehmen ist oder nicht, und bei deren Erforderlichkeit der fehlende Nachweis über die Durchführung dieser Datenschutz-Folgenabschätzung mit aller Wahrscheinlichkeit zu einem erhöhten Interesse an den betroffenen Verfahren. Dies kann dann wiederum zu vertieften Prüfungen seitens der Datenschutz-Aufsichtsbehörde mit der Folge weiterer Sanktionen führen.

Auch daher ist es wichtig, in den Unternehmen dafür Sorge zu tragen, dass alle nach derzeitigem Datenschutzrecht erforderlichen Vorabkontrollen durch den/die Datenschutzbeauftragte/n zeitnah durchgeführt werden und dem/der Datenschutzbeauftragten die hierfür erforderliche Zeit und Unterstützung zu gewähren.

3.4 Handlungsbedarf in den Unternehmen

Es ist zu prüfen, ob für alle Verfahren, für die bereits nach geltendem Recht eine Vorabkontrolle erforderlich ist, eine durchgeführt wurde und ob diese in ausreichendem Detailgrad dokumentiert wurden (Stichwort: Nachvollziehbarkeit des Ergebnisses)

Für alle Verfahren, bei denen die bereits nach geltendem Recht erforderliche Vorabkontrolle noch nicht durchgeführt wurde, sollte diese zeitnah (bis

spätestens 24. Mai 2018) nachgeholt und in ausreichendem Detailgrad dokumentiert werden.

Ab 25. Mai 2018 ist sicherzustellen, dass bei der Einführung neuer Verarbeitungstätigkeiten und bei wesentlichen Änderungen bestehender Verarbeitungstätigkeiten geprüft wird, ob eine Datenschutz-Folgenabschätzung erforderlich ist. Diese Entscheidung ist mitsamt dem Ergebnis der erforderlichen Datenschutz-Folgenabschätzung zu dokumentieren und bei Bedarf gegenüber der Datenschutz-Aufsichtsbehörde nachzuweisen.

Bei den Verarbeitungstätigkeiten, die von der Datenschutz-Aufsichtsbehörde in die Liste der Verarbeitungstätigkeiten bei denen eine Datenschutz-Folgenabschätzung durchzuführen ist (s.o.) aufgenommen wurde, ist diese mit hoher Priorität durchzuführen und zu dokumentieren.

4 Hilfsmittel zur Umsetzung (Auswahl)

- Das Standard-Datenschutzmodell (SDM) der Datenschutzaufsichtsbehörden
  - Zu finden unter: https://www.datenschutzzentrum.de/sdm/
- Whitepaper „DATENSCHUTZ-FOLGENABSCHÄTZUNG – Ein Werkzeug für einen besseren Datenschutz“ des Forum Privatheit
  - Zu finden unter: https://www.forum-privatheit.de – Publikationen und Downloads

1 In Art. 24 Abs. 2 DS-GVO ist „Anwendung geeigneter Datenschutzvorkehrungen“ als „Einführung und Umsetzung geeigneter Datenschutzregelungen und -strategien“ (engl.: „the implementation of appropriate data protection policies“ zu lesen.

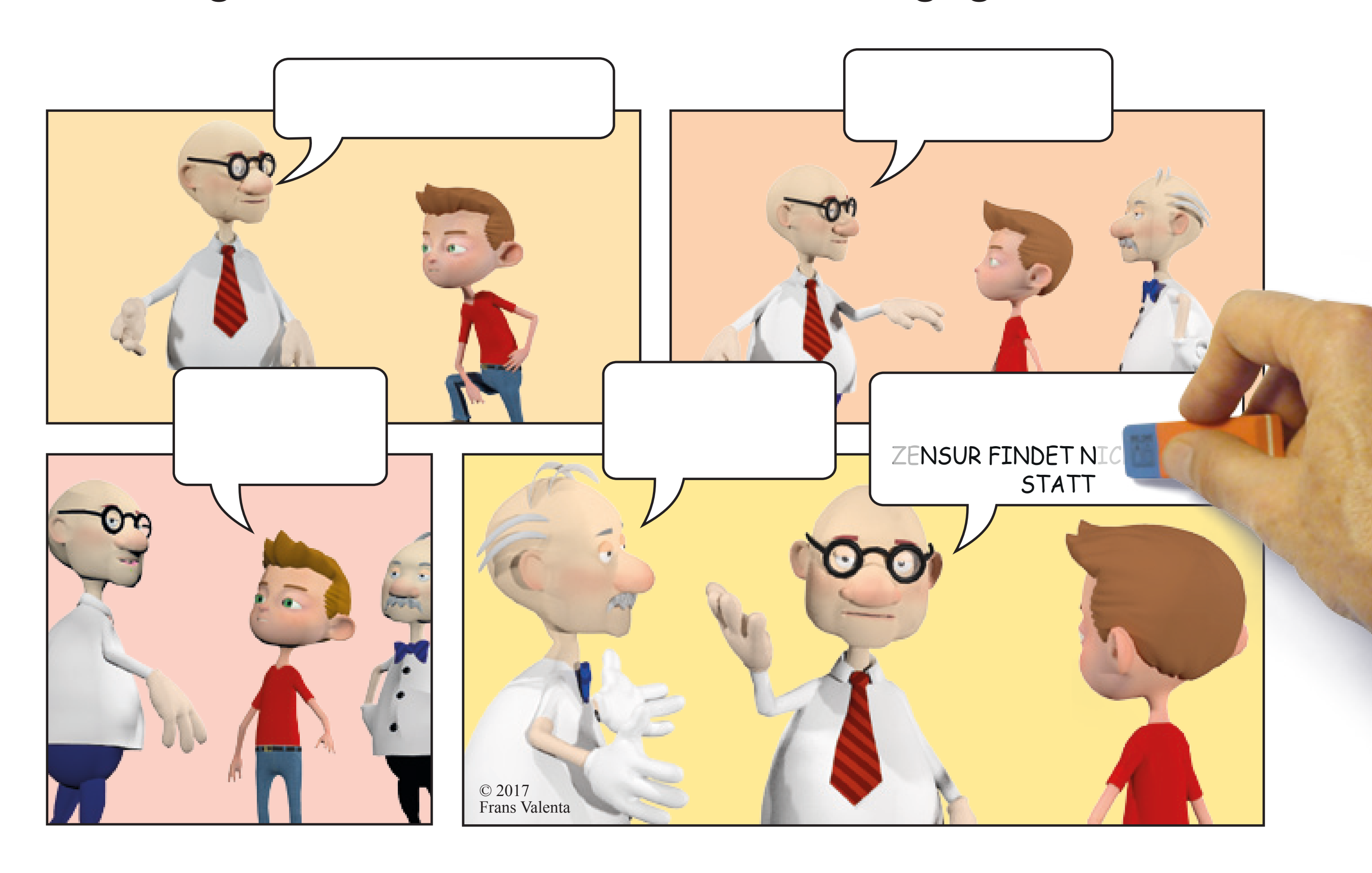
2 Der Erwägungsgrund 91 lässt sich im Gegensatz zu den anderen oben bei Absatz 1 genannten Erwägungsgründen direkt einem Absatz des Artikels zuordnen, daher ist der Erwägungsgrund 91 bei diesem Absatz genannt.

3 § 38 Abs. 1 Satz 2 BDSG-neu regelt, dass unabhängig von der Anzahl der Beschäftigten, die mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ein/e Datenschutzbeauftragte/r verpflichtend zu benennen ist, wenn ein Verantwortlicher oder ein Auftragsverarbeiter „Verarbeitungen vor[nimmt], die einer Datenschutz-Folgenabschätzung nach Art. 35 der Verordnung (EU) 2016/679 [das ist die DS-GVO] unterliegen“.

4 In der englischen Version steht hier „where appropriate“, dies wäre nicht mit „gegebenenfalls“ sondern mit „wenn es angebracht / angemessen / sachgemäß / zweckdienlich ist“ zu übersetzen.

Cartoon

Die Folgen des „Netzwerkdurchsetzungsgesetzes“



Thilo Weichert

Türkische Geheimdiensttätigkeit in Deutschland

Im Dezember 2016 veröffentlichte die regierungskritische türkische Zeitung Cumhuriyet Mails und Dokumente, die belegen, dass offensichtlich mehrere Imame, die in Moscheen des in Deutschland eingetragenen Vereins Ditib (Türkisch-Islamische Union der Anstalt für Religion, türkisch „Diyanet İşleri Türk İslam Birliği“) tätig sind, Informationen über vermutete Anhänger des Predigers Fethullah Gülen gesammelt haben. Am 05.05.2017 erhielt Ditib hierfür den deutschen Big Brother Award in der Kategorie Politik. Es gibt inzwischen Gründe genug, sich die geheimdienstliche Tätigkeit türkischer Behörden in Deutschland und die Reaktion deutscher Stellen hierauf etwas genauer anzusehen.

1 Der Putschversuch Juli 2016 und die Imame

Die Gülen-Bewegung, die von der türkischen Regierung Fetö (Fethullahistische Terrororganisation) genannt wird, wird von der türkischen Regierung für den Putschversuch am 15.07.2016 verantwortlich gemacht. Gülen-Anhänger gelten in der Türkei als Staatsfeinde, als Terroristen, die den Staat unterwandern. Nachweise, dass Gülen hinter dem Putsch stand, wurden bis heute von der türkischen Regierung nicht vorgelegt. Unter den 50 von Cumhuriyet veröffentlichten Listen finden sich Berichte der türkischen Generalkonsulate Köln und Düsseldorf; andere Berichte kommen aus München. Berichterstatter sind Ditib-Imame und Religionsattachés, die ihre eigenen Namen genauso vollständig nennen wie die Namen der Personen und Vereine, die sie denunzieren. Die Berichte gehen auf ein Schreiben der obersten türkischen Religionsbehörde vom 20.09.2016 zurück, in dem die Botschaften und Generalkonsulate aufgefordert werden, innerhalb einer Woche detaillierte Berichte über Organisationsstrukturen und Aktivitäten der Fetö zu schicken.

Das Material der Imam-Berichte landete u. a. bei einem Parlamentsausschuss in Ankara, der die Hintergründe des Putschversuchs gegen Staatspräsident Recep Tayyip Erdoğan aufklären soll. Ditib mit Sitz in Köln wird beschuldigt, insbesondere Gemeindemitglieder in Deutschland sowie deutsche Lehrer bespitzelt zu haben. Auftraggeber ist Diyanet, das Amt für religiöse Angelegenheiten in der Türkei, das praktisch direkt Präsident Erdoğan untersteht. Der religionspolitische Sprecher der Grünen, Volker Beck, hatte schon im Dezember Anzeige wegen Spionageverdachts gestellt. Diyanet hat ihre Bediensteten aufgefordert, Aktivitäten von Gruppen wie der Gülen-Bewegung zu melden. Die Aufforderung erging weltweit. Die Religionsattachés haben diese Order an die Imame der örtlichen Moscheegemeinden weitergegeben.

Die Imame der Ditib sind türkische Staatsbeamte und der Religionsbehörde Diyanet unterstellt. Ditib ist finanziell von der Religionsbehörde in Ankara abhängig. Der Präsident der Diyanet ist laut Satzung Ehrenvorsitzender der Ditib und Vorsitzender von dessen mächtigem Beirat. Der türkische Staat bestimmt mittelbar, wer in Deutschland für Ditib spricht. Wegen der informellen Einflussnahmen dürfte es keinen wichtigen Vorstandsposten in einer Ditib-Moschee geben, der nicht zuvor von Ankara bestätigt wurde.

Vor einigen Jahren noch hatte Diyanet dialogbereite und reformorientierte Moscheevorstände unterstützt. Inzwischen sind Reformer nicht mehr erwünscht. Im Sommer 2016 wurde der hessische Ditib-Landesvorsitzende Fuat Kurt abgewählt, der sich offen für den Dialog zeigte. In Berlin ist vor Weihnachten 2016 der gesamte Vorstand der Sehitlik-Moschee in Neukölln zurückgetreten – offenbar auf Druck des türkischen Generalkonsulats. Die Moschee galt als beispielhaft für ihre Offenheit. Der Ton in den Moscheegemeinden ist generell rauer geworden. Es wird geschätzt, dass die Mehrheit der Deutsch-Türken Erdoğans autokratischen Kurs unterstützen. Viele Gülen-Anhänger verlassen die Gemeinden.

2 Die misslungene Aufklärung

Ditib sprach zunächst nach Bekanntgabe der Spionage empört von „Unterstellungen“. Wenig später hieß es, die „schwerwiegenden Vorwürfe“ würden „sauber und transparent“ untersucht. Am 11.01.2017 wurde der Ditib-Generalsekretär Bekir Alboğa wie folgt zitiert: „Die schriftliche Anweisung des türkischen Religionspräsidiums Diyanet war nicht an die Ditib gerichtet. Trotzdem folgten dem einige wenige Ditib-Imame fälschlicherweise. Wir bedauern die Panne zutiefst und haben diesbezüglich auch mit Diyanet gesprochen.“ Einige Tage später dementierte Alboğa per Pressemitteilung sein Bedauern: Der Verband habe die „schwerwiegenden Vorwürfe der Bespitzelung nicht bestätigt“; mit dem Wort „Panne“ habe er nur gemeint, dass einige Imame die Direktiven aus Ankara „missverständlich ausgelegt“ hätten. Selbstverständlich würden von Imamen keine „Dienste außerhalb der religiösen Betreuung der Muslime erwartet“.

Mindestens 13 Imame aus Nordrhein-Westfalen stehen nach bisherigen Erkenntnissen des NRW-Verfassungsschutzes im Verdacht, Informationen über vermeintliche Gülen-Anhänger an den türkischen Staat weitergegeben zu haben. NRW-Verfassungsschutzpräsident Burkhard Freier teilte Anfang Januar 2017 im Innenausschuss des Düsseldorfer Landtags mit, es seien zumindest Informationen mit Namen von 33 bespitzelten Personen, davon fünf Lehrer, also deutsche Staatsbeamte, und elf

Institutionen aus dem Bildungsbereich an Diyanet geliefert worden. Für die Berichte an Ankara hätten auch Imame aus drei rheinland-pfälzischen Moscheegemeinden Informationen gesammelt. Ein Sprecher des Innenministeriums Nordrhein-Westfalen sagte: „Die betroffenen Personen sind – soweit sie anzutreffen waren – von den zuständigen Polizeibehörden in Gefährdeten-Ansprachen informiert worden.“ Man habe sie darauf aufmerksam gemacht, dass sie bei der Planung möglicher Türkeireisen beachten sollten, dass sie in den Berichten als Gülen-Anhänger aufgeführt seien.

Gemäß Berichten der Presse, der die Dokumente vorliegen, sind darin Details über Moscheebesuche enthalten. Eine Nachhilfeeinrichtung aus Bergneustadt wird als „Hort des Bösen“ gekennzeichnet. Im Vordergrund stehen Informationen über Verbindungen von Personen zur Gülen-Bewegung sowie zu deutschen Behörden. So heißt es in einem Bericht des Imam im rheinland-pfälzischen Fürthen über einen Mann: „Wahrt nach dem Putschversuch völlig unverändert seine Einstellung“ und über eine Frau: „Über sie wird gesagt, sie habe immer noch eine emotionale Bindung an die Bewegung. Sie ist Hausfrau“. Aus dem nordrhein-westfälischen Engelskirchen wurden die Namen von 16 Männern und Frauen einschließlich der Heimatorte in der Türkei weitergegeben, die Spenden für den „Fetö-Terror“ gesammelt hätten. Aus den Berichten kann geschlossen werden, dass die Spitzelei schon seit längerer Zeit praktiziert wird.

Tatsächlich wurden aus 35 Ländern Berichte abgeliefert, u. a. aus Nigeria, Mauretanien, Tansania, Kenia, Saudi-Arabien, der Mongolei oder Australien. Spitzelberichte gab bzw. gibt es nicht nur aus Deutschland, sondern auch aus anderen europäischen Ländern wie Österreich, der Schweiz, Dänemark, Belgien und den Niederlanden. Übermittelt wurden dabei nicht nur Namen von Personen, sondern auch Hinweise auf Schulen, Kitas, Kultur- und Studentenvereine, die angeblich von der Gülen-Bewegung betrieben werden. In Österreich warnten die Verfasser vor einer „Unterwanderung“ durch die „Fetö“. Die Botschaft Bern mutmaßte, „gewaltbereite Aktivisten“ der Gülen-Bewegung seien aus der Türkei geflohen und hätten sich in der Schweiz „festgesetzt“.

3 Staatsanwaltliche Ermittlungen

Am 15.02.2017 durchsuchte die Polizei in Nordrhein-Westfalen und Rheinland-Pfalz die Wohnungen von vier Geistlichen, die in Ditib-Gemeinden predigen, wegen des Verdachts der geheimdienstlichen Agententätigkeit. Die Razzien wurden vom Generalbundesanwalt in Auftrag gegeben. Eine Sprecherin der Bundesanwaltschaft teilte mit, dass das sichergestellte Material, darunter Kommunikationsmittel, Datenträger und schriftliche Unterlagen, umgehend ausgewertet wird. Festnahmen hat es keine gegeben. Die Bundesanwaltschaft ermittelte konkret gegen 16 Personen wegen des Verdachts des Verstoßes gegen § 99 Strafgesetzbuch (StGB). Dieser Paragraph verbietet das Sammeln und Mitteilen von „Tatsachen, Gegenständen oder Erkenntnissen“ für „Geheimdienste einer fremden Macht“.

Gemäß Presseberichten waren die polizeilichen Durchsuchungen eigentlich schon für Ende Januar geplant. Ein Sprecher der Bundesanwaltschaft sagte auf Anfrage, damals seien auch Haftbefehle beantragt worden. Der Ermittlungsrichter des Bundesgerichtshofs (BGH) habe bislang aber nicht den dafür notwendigen dringenden Tatverdacht gesehen.

Die Beschuldigten wurden bei den Durchsuchungen nicht angetroffen. Sie hatten sich offensichtlich in die Türkei abgesetzt. Am 17.02.2017 teilte Diyanet über ihren Präsidenten Mehmet Görmez in Ankara mit, sie habe sechs unter Spionageverdacht stehende Imame in die Türkei zurückbeordert, was von Ditib als disziplinarische Maßnahme dargestellt wurde. Diese hätten ihre Kompetenzen überschritten, sich aber nicht strafbar gemacht: „Es gibt keine Spionagetätigkeit.“ Die Rückkehr in die Türkei sei ein Zeichen des guten Willens. Die „Kampagne“ in Deutschland gegen die Diyanet und gegen Ditib seien inakzeptabel. Anfang Mai 2017 waren von den 16 Beschuldigten zehn in die Türkei zurückbeordert und so der effektiven deutschen Strafverfolgung entzogen.

Während die deutschen Strafverfolgungsbehördenweiter ermitteln, erklärte der Ditib-Abteilungsleiter für Außenbeziehungen, Zekeriya Altug, die Affäre intern für aufgeklärt. Ditib-Imame hätten in 10 bis 15 Fällen Berichte über vermeintliche Gülen-Anhänger nach Ankara weitergeleitet. Angesichts der 900 Moscheegemeinden sei dies eine geringe Zahl; ein „strukturelles Problem“ gebe es nicht. In den Gemeinden hätten Menschen aller Couleur Platz, auch Anhänger von Milli Görüs und von Gülen: „Wir wollen die Vielfalt in den Gemeinden erhalten.“

Ditib teilte anlässlich der polizeilichen Durchsuchungsaktion mit, es handele sich bei den durchsuchten Wohnungen um Privatwohnungen, nicht um Ditib-Vereinsräume: „Die Ermittlungen richten sich nicht gegen den Ditib-Verband, nicht gegen Ditib-Mitarbeiter und auch nicht gegen die Ditib-Moscheen“. Tatsächlich wird Ditib in der Pressemitteilung der Bundesanwaltschaft nicht explizit erwähnt, wohl aber die Religionsbehörde Diyanet, die die Imame von der Türkei in die Ditib-Gemeinden entsendet.

Am 13.03.2017 leitete die Generalbundesanwaltschaft zusätzlich zu den 16 Ditib-Verfahren ein Ermittlungsverfahren gegen Halife Keskin ein, ein hochrangiger Funktionär der Diyanet, der diplomatische Vertretungen weltweit aufgefordert hatte, Informationen über die Gülen-Bewegung zu sammeln. Den Ermittlern sollen von einem Insider reichlich Unterlagen zugespielt worden sein.

4 Reaktionen

Die Integrationsbeauftragte der Bundesregierung Aydan Özoğuz (SPD) forderte Konsequenzen aus der Spionageaffäre: „Die Spitzelvorwürfe gegen Ditib sind gravierend. Es ist gut, dass der Generalbundesanwalt jetzt Ermittlungen aufgenommen hat. Özoğuz fordert, dass sich Ditib „glaubhaft von Ankara löst. Ein erster zwingender Schritt muss die Änderung der Satzung sein, die die enge Verbindung zur türkischen Religionsbehörde Diyanet festschreibt“.

Die Migrationsbeauftragte der Linken-Bundestagsfraktion Sevin Dağdelen forderte konkrete Maßnahmen gegen die denunzierenden Imame: „Erdoğans Spitzel müssen umgehend ausgewiesen werden.“ Die Kooperation mit Ditib sei

zu beenden. Grünen-Religionsexperte Beck kritisierte Bundesregierung und deutsche Behörden, die seiner Auffassung nach zu spät mit den Ermittlungen gegen den Verband begannen. Selbst nach seiner Anzeige von Mitte Dezember 2016 sei zunächst gar nichts passiert. Die tatverdächtigen Imame und Religionsattachés hätten dadurch genügend Zeit gehabt, unbehelligt in die Türkei zurückzukehren. Beck warf der Bundesregierung weiter vor, sie habe aus Rücksicht auf das Flüchtlingsabkommen mit der Türkei so gehandelt.

Justizminister Maas sieht in Reaktion auf die Razzien für einen Zusammenarbeit mit Ditib keine Zukunft, wenn der Verein sich nicht von Ankara loslöst. Der Einfluss des türkischen Staates auf Ditib sei zu groß. Er forderte Ditib auf, seine Satzung zu ändern, die die enge Verbindung zur türkischen Religionsbehörde Diyanet festschreibt. Der Verband müsse sich glaubhaft von Ankara lösen: „Nur als unabhängiger deutscher Verband hat Ditib eine Zukunft als verlässlicher Partner.“ Maas verlangte von Ditib, dass die Spionage-Vorwürfe „unverzüglich und lückenlos“ aufgeklärt werden. Wer den Islam als Deckmantel für Spionage benutze, könne sich nicht auf die Religionsfreiheit berufen. Auch das Bundesinnenministerium rief Ditib auf, den Vorwurf der Bespitzelung aufzuklären. Innenstaatssekretär Ole Schröder (CDU) meinte, die Bundesländer müssten prüfen, ob Ditib die Voraussetzungen für eine Religionsgemeinschaft erfülle. Es müsse möglicherweise auch untersucht werden, ob der Sonderstatus, den Imame genössen, gerechtfertigt sei.

Mustafa Yeneroğlu, Mitglied der türkischen Regierungspartei AKP und Vorsitzender des sog. Menschenrechtsausschusses im türkischen Parlament, ging Maas für seine Kritik scharf an: „Ich verurteile die Razzien gegen Ditib-Imame auf das Schärfste. Unter dem Deckmantel eines rechtlich unhaltbaren Spionagevorwurfs wird eine beispiellose Einschüchterungskampagne gegen die mitgliederstärkste islamische Religionsgemeinschaft in Deutschland gefahren und die öffentlichen Erklärungen von Bundesjustizminister Maas offenbaren die eigentliche politische Motivation hinter der Aktion.“ Yeneroğlu sieht auch hinter dem Zeitpunkt der Razzien politische Beweggründe: „Nicht nachvollziehbar ist zudem, warum der Generalbundesanwalt die Wohnungsdurchsuchungen mehrere Wochen nach Beginn der Ermittlungen anordnet. Auch dies spricht dafür, dass es sich hierbei nicht um eine juristisch notwendige Maßnahme handelt, sondern um eine politische. Offenbar wollte man den Türkei-Besuch von Bundeskanzlerin Angela Merkel nicht belasten.“ Dieser war kurz vorher durchgeführt worden.

Der Präsident der Religionsbehörde Mehmet Görmez wies die Spionage-Vorwürfe entschieden zurück. Ditib bemühe sich in Deutschland, die Gläubigen vor einem falschen Religionsverständnis zu schützen. Er sei „sehr traurig“ darüber, dass die Bemühungen, die Moscheegemeinde in Deutschland zu schützen, als Spionagetätigkeit bezeichnet werden. Ditib arbeite seit Jahrzehnten auf der „Grundlage des Rechts“. Für ihn sei nicht vorstellbar, dass der Moscheeverein Recht ignoriere. Ein Schreiben seiner Behörde sei nicht an die Imame oder Moscheen gerichtet gewesen. Dennoch werde seine Behörde jeder Behauptung nachgehen und unternehmen, was nötig sei, wenn „einzelne individuelle Fehler“ passiert seien. Er frage sich jedoch, ob die Reaktionen in Deutschland so ausfallen würden, wenn es nicht um die Gülen-Bewegung, sondern um die Terrormiliz IS gehen würde.

Der türkische Justizminister Bekir Bozdağ verurteilte die polizeilichen Durchsuchungen als „klaren Verstoß gegen internationale Abkommen und die deutsche Verfassung“. Schließlich sei die Religions- und Glaubensfreiheit dort festgeschrieben, sagte er unter Verweis auf Grundgesetz und Abkommen. Bozdağ, der der regierenden AK-Partei angehört, warf den deutschen Behörden indirekt vor, unter dem Einfluss der Gülen-Bewegung zu handeln. Die Ermittlungen zeigten, wie leicht Deutschland „den Behauptungen von Terroristen Glauben schenkt“.

Der Vorsitzende der Kurdischen Gemeinde in Deutschland, Ali Ertan Toprak, meinte dagegen, wer mit der Ditib zusammenarbeite – wie es viele Landesregierungen nicht nur beim islamischen Religionsunterricht tun –, der lege die Zukunft der deutschen Muslime in die Hände des türkischen Präsidenten Erdoğan. Er warnte vor türkisch-nationalistischen „Gegengesellschaften“, die aggressiv gegen westliche Werte vorgingen. Das Klima in der türkischen Gemeinde in Deutschland sei vergiftet. Erdoğan-Anhänger denunzierten Nachbarn und Kritiker des türkischen Präsidenten.

Am 05.05.2017 wurde in Bielefeld im Rahmen einer öffentlichen Festveranstaltung Ditib der Big BrotherAward 2017 in der Kategorie „Politik“ verliehen. Auf die Einladung zu dieser Veranstaltung hin reagierte Generalsekretär Alboğa mit einem zweiseitigen Antwortschreiben, in dem er betonte, Ditib habe mit der „Spitzel-Affäre“ nichts zu tun. Die Vorwürfe fußten auf „Tatsachenverdrehung, Falschbehauptung und unzulässigen Verallgemeinerungen“. Er bat um „umgehende Revidierung“ des „Urteils“ und wies darauf hin, dass, sollte dem nicht gefolgt werden, „eine Strafbarkeit nach § 186 Strafgesetzbuch in Betracht kommen würde.“

Die rot-grüne NRW-Regierung verlangte eine lückenlose Aufklärung der Vorwürfe und forderte eine strikte Trennung von Ankara. Davon soll abhängig gemacht werden, ob die Zusammenarbeit mit der Ditib fortgesetzt wird. NRW-Sozialminister Rainer Schmeltzer (SPD) sagte, er erwarte von Ditib den „ernsthaften Willen zur Loslösung vom direkten Einfluss türkisch-staatlicher Institutionen“. Signale sollten bald erfolgen, die Umsetzung der Verselbständigung brauche aber Zeit. Er wolle aber weiter mit Ditib reden. Das Zentralkomitee der deutschen Katholiken (ZdK) plädierte dafür, den Dialog mit Ditib einstweilen fortzusetzen, so ZdK-Präsident Thomas Sternberg: „Ich kann nur davor warnen, bereits jetzt die gesamte Ditib in Verruf zu bringen“.

5 Ditib

Direkt nach dem Putschversuch im Juli 2016 war die 1984 gegründete Ditib schon einmal in die Kritik geraten, weil in einigen der Moscheegemeinden Gülen-Anhänger vom Gebet ausgeschlossen wurden und in den direkt aus Ankara kommenden Predigten gegen sie gehetzt wurde. Ditib ist mit Abstand die größte muslimische, weiter wachsende Organisation in Deutschland, sie vertritt 15

Landes- und Regionalverbände sowie gut 900 Gemeinden. Der Dachverband richtet sich inhaltlich strikt an den Vorgaben aus Ankara aus, ihr Vorstandsvorsitzender wechselt häufig.

Die Ditib-Imame sind aus Ankara abgeordnete und bezahlte Beamte der türkischen Religionsbehörde Diyanet. Auch die sogenannten Religionsbeauftragten in jeder Gemeinde beziehen laut einem Ditib-Sprecher ihr Gehalt aus Ankara. Zudem sitzen gemäß der Vereinssatzung in allen wichtigen Ditib-Gremien Diyanet-Vertreter. Außerdem ist der Vorstandsvorsitzende von Ditib traditionell der Religionsattaché der türkischen Botschaft in Berlin. Der Politikwissenschaftler an der Universität Ankara Baskin Oran meinte, Erdoğan betrachte Ditib als ein Instrument, um seine Herrschaft über die Türkei hinweg auszudehnen: „Die Regierung macht das in der Türkei genauso. Das System Erdoğan beruht auf Spionage."

Trotzdem galt Ditib dem deutschen Staat lange als verlässlicher Dialogpartner, wenn es um die Integration der Muslime ging, um islamische Lehrstühle oder den Religionsunterricht. Man sah zu Ditib keine Alternativen. In Deutschland sind die christlichen und jüdischen Gläubigen in großen Kirchen organisiert. Bei den Muslimen ist das Bild sehr viel zersplitterter, zumal die Muslime in Deutschland die unterschiedlichsten Herkunftsländer haben. Da Muslime aus der Türkei die größte Gruppe stellen und Ditib dem Modell einer organisierten Kirche am nächsten kommt, lag es nahe, den Verein als Ansprechpartner zu wählen. Die von Ditib angestrebte Anerkennung als Religionsgemeinschaft ist mit den Spionagevorwürfen in weite Ferne gerückt.

In Hamburg und Bremen wurden zunächst Staatsverträge mit Ditib geschlossen, die den islamischen Religionsunterricht an Schulen regeln. Seit dem Bekanntwerden der politischen Instrumentalisierung wurde die Skepsis hierzu immer größer. In Hessen ist Ditib ebenfalls der Ansprechpartner für den islamischen Religionsunterricht. Das dortige Kultusministerium prüft nun, ob Ditib unabhängig vom türkischen Staat sei. In Niedersachsen stand man kurz vor einem Abkommen – seit den Vorwürfen nach dem Putsch liegen die Verhandlungen auf Eis.

Auch in NRW gibt es einen Beirat, der sich mit dem islamischen Religionsunterricht beschäftigt. Der Ditib-Vertreter lässt seinen Sitz dort nach dem Beginn der Ermittlungen ruhen. Bei einem Präventionsprojekt gegen Salafismus hat die Landesregierung die Zusammenarbeit aufgekündigt, nachdem Diyanet einen Comic herausgegeben hatte, in dem ein Vater seinen Sohn über die Schönheit des Märtyertods aufgeklärt: „Märtyrer sind im Himmel so glücklich, dass sie zehnmal Märtyrer sein wollen". Ditib hatte hierzu erklärt, dass dafür nicht der Verein, sondern Diyanet verantwortlich zeichnete. Dass dies formaljuristisch auch in Bezug auf das Arbeitsrecht gilt, entschied Anfang April 2017 das Arbeitsgericht Köln: Zwei türkische Imame klagten gegen Ditib auf Wiedereinstellung an deutschen Ditib-Moscheen in Südbaden, wo sie nach dem gescheiterten Putsch entlassen worden waren. Das Arbeitsbericht entschied, es habe kein Arbeitsverhältnis mit dem Verband bestanden; die Seelsorger seien Beamte des türkischen Staates gewesen. Sie hätten zwar in den Moscheen gearbeitet und gewohnt, aber nicht belegen können, dienstliche Weisungen von Ditib erhalten zu haben. Die klagenden Imame haben Asyl in Deutschland beantragt.

Obwohl die Spionage-Ermittlungen gegen Imame von Ditib andauerten und sich die Einsicht von Ditib über die Unvereinbarkeit des Vorgehens der Imame mit einer freiheitlichen Kultur in Grenzen hielt, wurde Anfang Mai 2017 bekannt, dass die Bundesregierung den muslimischen Verband wieder mit mehr als einer Million Euro fördern möchte. Das Bundesfamilienministerium will bereits bewilligte Gelder u. a. für Integrationskurse und Projekte mit Jugendlichen, die aufgrund der Vorwürfe zurückgehalten wurden, auszahlen, weil Ditib-Vertreter eine „strikte Trennung zwischen den geförderten Modellprojekten sowie den vom Ermittlungsverfahren Betroffenen" zugesichert haben.

6 Türkische Spitzel in Deutschland

Bereits im Sommer 2016 war bekannt geworden, dass die türkische „Nationale Geheimdienst-Organisation" (MIT) in Deutschland ca. 6.000 Informanten beschäftige. Die deutschen Sicherheitsbehörden gehen davon aus, dass in Deutschland rund 150 MIT-Mitarbeiter an der türkischen Botschaft und an den Konsulaten arbeiten. Eine interne Analyse aus dem Bundesinnenministerium vom Oktober 2016 schrieb: „Es muss ermittelt werden, ob und inwieweit der türkische Geheimdienst MIT mittels nachrichtendienstlicher Einflussoperationen versucht, getarnt in die Willensbildung von deutschen Institutionen einzugreifen und die öffentliche Meinung unter anderem durch Desinformation zu lenken." In einem vertraulichen Lagebericht des Auswärtigen Amtes vom Febraur 2017 heißt es: „Der MIT ist die Institution, die am meisten Einfluss gewinnen konnte." Der Grünen-Bundestagsabgeordnete Hans-Christian Ströbele, Mitglied im Parlamentarischen Kontrollgremium, das die deutschen Nachrichtendienste überwacht, forderte die Bundesregierung und die Sicherheitsbehörden auf, die bespitzelten Bürger zu beschützen. Solche Denunzierungen wie die durch die Ditib-Imame seien schwere Straftaten.

Anfang 2017 wurde über die Presse bekannt, dass die türkischen Behörden auch die türkischen Migranten zum Ausspionieren einzusetzen versuchen. Gemäß Informationen der Gewerkschaft Erziehung und Wissenschaft (GEW) sollen türkischstämmige SchülerInnen von den türkischen Konsulaten in Nordrhein-Westfalen aufgefordert worden sein, ihre Lehrkräfte heimlich zu filmen. Wenn diese Kritik am Regime um Staatschef Erdoğan äußern, sollten die SchülerInnen – in Deutschland, nicht in der Türkei – die Aufnahmen an die türkischen Behörden weiterleiten. Hierzu habe es in den Konsulaten des Landes entsprechende Info-Veranstaltungen für Lehrer- und Elternvereine gegeben. GEW-Landesvorsitzender Sebastian Krebs teilte mit: „Wir haben aus unterschiedlichen Quellen erfahren, dass die Teilnehmer dazu angehalten wurden, den Generalkonsulaten jede Kritik an der türkischen Regierung, die in NRW-Schulen beobachtet wird, zu melden".

Die Kooperation deutscher mit türkischen Stellen bringt rechtsstaatliche Konflikte mit sich. Dies zeigt ein Strafverfahren gegen zehn türkischstämmige Kommunisten vor dem Oberlandesgericht München, in dem geklärt werden

soll, ob es sich, wie von der türkischen Regierung behauptet, bei der linksextremen Splittergruppe Kommunistische Partei der Türkei/Marxistisch-Leninistisch (TKP/ML) um eine Terrororganisation handelt. Dabei verwendet die anklagende Bundesanwaltschaft türkische Geheimdienst-Informationen vom September 2013, wonach die TKP/ML angeblich in Deutschland einen 700 bis 800 Personen starken Kader mit bis zu 2.000 SympathisantInnen habe und dann stolz Namen, Daten und Anschriften der Personen auflistet, „die nach Einschätzung in den zirkulierenden geheimdienstlichen Informationen“ hier aktiv seien. Nach Ansicht von Peer Stolle, Verteidiger einer angeklagten türkischstämmigen Ärztin, sind diese Beweismittel rechtsstaatswidrig in Deutschland erlangt worden. Die schwarze Ironie des Vorgangs bringt es mit sich, dass die Informationen vom früheren Direktor der türkischen Abteilung für Terrorbekämpfung Ömer Köse stammt, der inzwischen seit zwei Jahren wegen des Vorwurfs der Dokumentenfälschung, der illegalen Telefonüberwachung, der Verletzung der Privatsphäre, der Beweisfälschung und der Preisgabe von Ermittlungsinformationen in der Türkei in Haft sitzt.

Der Prozess gegen TKP/ML, der im Sommer 2016 begann, soll sich noch mindestens bis 2018 hinziehen. Angesichts der aktuellen Erkenntnisse über die türkischen Spionageaktivitäten in Deutschland beantragten die Verteidiger, die Verfolgungsermächtigung gegen die 10 Angeklagten zurückzunehmen. Dann würde der Prozess platzen. Ende März 2017 entschied sich die Bundesregierung dagegen, worauf die Verteidiger Strafanzeige wegen der türkischen Spionage erstatteten.

Das MIT-Engagement geht über die Beobachtung der Opposition im Ausland hinaus. So wurde in Hamburg ein mutmaßlicher MIT-Agent festgenommen, der Morde an Kurdenvertretern in Deutschland und Belgien geplant haben soll. In Frankreich kamen Ermittler nach dem Mord an drei kurdischen Aktivistinnen 2013 zum Schluss, dass die MIT an der Vorbereitung der Gewalttat beteiligt war.

Lange Zeit haben sowohl die deutsche wie auch die türkische Seite versucht, Konflikte möglichst geräuschlos beizulegen. Das ist aber immer weniger möglich, nachdem sich zeigt, dass die Türkei friedliche Regierungskritiker wie z. B. den deutsch-türkischen Welt-Journalisten Deniz Yücel inhaftiert und zu Terroristen erklärt und, wie am 06.03.2017 der türkische Justizminister Bekir Bozdağ, deutschen Behörden Nazi-Praktiken vorwarf. Im Vorlauf zum Referendum über die Autokratisierung der Türkei am 16.04.2017 wurde der Nazivorwurf zum klassischen Propaganda-Muster der türkischen Regierung und regelmäßig insbesondere auch von Präsident Erdoğan verwendet. Dies fiel bei vielen offenbar auf fruchtbaren Boden, stimmten doch 63,1% der Auslandstürken in Deutschland – bei einer Beteiligung von 46% – für die Verfassungsänderung.

7 Das Dossier des MIT

Die Türkei benutzte ihre geheimdienstlichen Aktivitäten gezielt, um die politische Führung in Deutschland zu provozieren und dadurch die identitäre Stimmung in der türkischen Community zu schüren mit dem Kalkül, dadurch Stimmen für das Referendum zugunsten der türkischen Verfassungsreform zu mobilisieren.

Hartes Geschütz fuhren die türkischen Behörden auf, als der 48-jährige Chef des türkischen MIT Hakan Fidan am Rande der 53. Münchener Sicherheitskonferenz vom 17. bis 19.02.2017 dem Präsidenten des Bundesnachrichtendiensten Bruno Kahl ein Dossier mit der Bitte um Amtshilfe überreichte. Kahl solle die Liste an den Verfassungsschutz übergeben. Der wäre ja für so etwas zuständig. Darin befand sich eine 69 Seiten umfassende Tabelle mit Namen und Einrichtungen, auf jeder Seite gekennzeichnet mit „freigegeben für die Bundesrepublik Deutschland“. In einer Art Vorwort wurde beklagt: „Es kann ausgesagt werden, dass die deutschen Dienststellen die Türkei bei dem begonnenen Vorgehen gegen die FETÖ/PSS nicht im erwarteten Ausmaß unterstützen.“ PSS steht für „Parallele Staatsstrukturen“. In dem Dossier wird behauptet, dass die Gülen-Bewegung seit 1990 in Deutschland aktiv sei und eine „verwurzelte Organisierung“ besitze mit „Firmen, wirtschaftlich-kommerziellen Betrieben, Vereinen, Stiftungen, Kulturzentren, Denkeinrichtungen, Medien- und Bildungsinstitutionen“. Deren „Aktivitäten“ hätten sich in Deutschland „enorm beschleunigt“; Deutschland werde, so das Dossier, von Gülen „zu einem zentralen Stützpunkt in Europa“ ausgebaut, verbunden mit dem Hinweis auf türkische NATO-Militärangehörige und Diplomaten, die nach der beispiellosen Verfolgungsaktion in Reaktion auf den Putschversuch in Deutschland Asyl beantragt haben.

Die Botschaft des Dossiers: Deutschland beherbergt Staatsfeinde. Mehr als 300 Namen und 200 Einrichtungen stehen auf der Liste: Imame, JournalistInnen, Vorsitzende von Bildungsvereinen. Je sechs Namen finden sich auf einer Seite des Dossiers, oft versehen mit Mail-Adresse, Handynummer, Wohnanschrift und Foto. Manchmal findet sich der vorsorgliche Hinweis, die Person könne womöglich einen Asylantrag in Deutschland stellen, oder, dass jemand der „kleine Bruder“ von wem ist. Aufgelistet werden zudem Hunderte Firmen, Taxibetriebe und eine Fahrschule, Steuerberatungskanzleien und Immobilienbetriebe, Restaurants und Dönerbuden.

In einer der Tabellen finden sich 83 Dialogzentren, Wirtschaftsverbände und Kulturvereinigungen; zwölf Zeitungen, Verlage und Fernsehsender sind gelistet und sehr viele Schulen, selbst Kindergärten. Unter der Rubrik „Machtzentren und Nichtregierungsorganisationen“, mit denen die Gülen-Bewegung „gute Beziehungen“ aufgebaut habe, werden die aus dem Ruhrgebiet stammende SPD-Politikerin Michelle Müntefering und die Berliner CDU-Politikerin Emine Demirbüken-Wegner, einstmals Staatssekretärin in der Berliner Landesregierung und Mitglied des CDU-Bundespräsidiums, aufgeführt. Weiterhin erwähnt wird der Name eines früheren Redenschreibers von Helmut Schmidt und heutigen Journalisten, der sich für die Gülen-Bewegung starkgemacht habe.

8 Nur dezente Absetzbewegungen

BND-Präsident Kahl informierte die Bundesregierung. Das Bundesamt für Verfassungsschutz verteilte das Dossier am 03.03.2017 an alle Länder. Dort gab es keine Abstimmung; die Bundesbehörden gaben sich insofern auch keine

Mühe. Es verstrichen Wochen, bis die Betroffenen informiert wurden. Als erste Länder wurden Niedersachsen und Nordrhein-Westfalen mit Warnungen an die Betroffenen aktiv; die anderen Bundesländer zogen nach. Der Generalbundesanwalt erhielt auch die Liste mit dem Hinweis, das Material sei nicht gerichtsverwertbar, könne also auch nicht für Ermittlungen genutzt werden. Nach der Veröffentlichung des Vorgangs nahm er aber Ermittlungen wegen des Verdachts der Spionage gegen Unbekannt auf. Eine Sprecherin des Generalbundesanwalts erklärte: „Der Erfolg unserer Ermittlungen wird wesentlich von den Erkenntnissen abhängen, die uns von den deutschen Spionage-Abwehrbehörden mitgeteilt werden".

Der Chef der Gülen-Bewegung in Deutschland, Ercan Karakoyun brachte seine Sorge zum Ausdruck: „Die Existenz dieser Liste macht mir Angst." Der Vorsitzende der SPD-Bundestagsfraktion Thomas Oppermann bezeichnete es als „absolut unerträglich", dass Abgeordnete ins „Visier des türkischen Geheimdienstes" geraten seien. Ankara müsse dafür sorgen, dass „diese Bespitzelung" sofort aufhöre. Bundesinnenminister Thomas de Maizière erklärte: „Spionageaktivitäten auf deutschem Boden sind strafbar und werden von uns nicht geduldet. Es kann nicht sein, dass diejenigen, die der Türkei irgendwie missliebig sind, Sorge haben müssen, in die Türkei zu fahren".

Teile der CDU reagierten mit der Forderung nach einem „Islamgesetz" auf die Veröffentlichungen, so u. a. die stellvertretende Parteivorsitzende Julia Klöckner, das Präsidiumsmitglied Jens Spahn oder der Vorsitzende der Mittelstands- und Wirtschaftsvereinigung der Union (MIT) Carsten Linnemann, der meinte: „Der Staat muss wissen, wo Moscheen sind und was in ihnen passiert. Wenn dort kein deutsch gesprochen wird und ein radikaler Islam gepredigt wird, muss Integration scheitern." Klöckner assistierte: „Ein Islamgesetz kann die Rechte und Pflichten der Muslime in Deutschland auf eine neue rechtliche Basis stellen." Die Forderung nach einem Islamgesetz wurde nicht nur von der Opposition, sondern auch von der SPD, von Kirchenvertretern sowie von Bundesinnenminister de Maizière zurückgewiesen.

9 Deutsch-türkische Geheimdienstbeziehungen

In einem Lagebericht des Auswärtigen Amtes zur Türkei vom Februar 2017 heißt es: „Die Regierung hat seit dem Putschversuch seine fast alles beherrschende nationalistische Atmosphäre geschaffen, die gleichermaßen auf Furcht, Euphorie, Propaganda und nationale Einheit setzt". Dessen ungeachtet versucht die deutsche Diplomatie, den Draht zu den türkischen Sicherheitsbehörden nicht abreißen zu lassen. Man braucht diese für die Bekämpfung des sog. Islamischen Staats (IS). Man ist froh, dass die Türkei die Grenze zu Syrien abgeriegelt hat und kontrolliert, wer als Rückkehrer unterwegs ist. Diese Zusammenarbeit soll auch richtig gut funktionieren.

Während früher die Erwartungen der türkischen Seite gegenüber den deutschen Behörden sich auf die AnhängerInnen der Kurdischen Arbeiterpartei PKK konzentrierten, hat sich das Anforderungsprofil massiv erweitert und erfasst insbesondere die Gülen-AnhängerInnen. Erst 2016 begann das Bundesamt für Verfassungsschutz zu prüfen, ob AKP-nahe private Vereine die Spitzeltätigkeit des MIT unterstützen.

Geheimdienstliche Kooperationen spielen sich nicht nur jenseits der öffentlichen Wahrnehmung, sondern auch oft jenseits des Rechts ab. Es herrscht ein Geben und Nehmen. Diplomatie geht vor „Rule of Law". Inwieweit nicht nur politische und wirtschaftliche Interessen in die Geheimdienstarbeit wie auch in die behördliche Reaktion auf fremde Spionage in Deutschland einfließen, sondern auch die Rücksicht auf die Menschen und die Menschenrechte, ist von der Transparenz und der öffentlichen Diskussion abhängig. Deutschland ist keine Insel der Seligen, auf der die Grundrechte und insbesondere auch der Schutz vor Ausforschung und informationeller Diskriminierung und Verfolgung geschützt werden, sondern zugleich politischer Partner von Staaten, für die Diskriminierung und Verfolgung systembedingt sind. Gegen derartige Partnerschaften ist grds. nichts einzuwenden, da der Austausch über Grundrechte und Freiheiten mit solchen Staaten einen generellen Austausch bedingt. Notwendig bleibt aber in jedem Fall die Prüfung, wem dieser Austausch mehr hilft, der Förderung von Grundrechten und Demokratie oder deren Beseitigung. Diese schwierige Prüfung kann nur über eine öffentliche kontroverse Debatte erfolgreich sein. Sie setzt – bei aller Kompromissbereitschaft bei konkreten Vorgängen – ein kompromissloses Bekenntnis zu informationellen Grundrechten voraus. Insofern gibt es Einiges zu tun – auch und gerade in Deutschland.

Verwendete Quellen: Hür, DITIB-Imame spionierten offenbar in Deutschland, www.deutschlandfunk.de 12.12.2016; Spitzelvorwurf gegen Ditib, SZ 13.01.2017, 6; Burger, Spionage und weitere Pannen, www.faz.net 13.01.2017; Drobinski, Risse, die tiefer werden, SZ 14./15.01.2017, 6; Imame unter Spionageverdacht, SZ 19.01.2017, 5; Ramelsberger, Namen, Daten, Anschriften – alles ausspioniert, SZ 24.01.2017, 5; Drei Listen mit 28 Namen, SZ 25.01.2017, 6, „Von Ankara lösen", Der Spiegel 4/2017, 25; Spion im Nebenjob, SZ 04./05.02.2017, 6; Aykanat/Bielicki/Drobinski, Spionageverdacht bei Ditib: Polizei durchsucht Wohnungen von Imamen, www.sueddeutsche.de 15.02.2017; Beweise bei türkischen Imamen gefunden, www.handelsblatt.com 15.02.2017; Türkische Politiker toben nach Ditib-Razzia und lassen schlimmen Vorwurf anklingen, www.focus.de 16.02.2017; Imame zurück in der Türkei, SZ 18./19.02.2017, 6; Baumgärtner/Caylan/Diehl/Elger/Knobbe/Popp/Schindler/Schmid/Schmidt/Schmidt, Tarnung Imam, Der Spiegel 8/2017, 28 ff.; Güsten, Mehr als 6.000 Spitzel in Deutschland, http://www.das-parlament.de/2017/9_10/themenausgaben/-/495026: Moritz, Der Spion im Klassenzimmer, www.handelsblatt.com 22.02.2017; Mascolo/Pinkert/Steinke, Der Irrtum des Top-Spions, SZ 28.03.2017, 6; Mascolo, De Maizière: Türkische Spionage wird nicht geduldet, SZ 29.03.2017, 1; Leyendecker/Mascolo, Deutsche Politiker auf Ankaras Geheimdienst-Liste, Staatsfeinde auf 69 Seiten, SZ 30.03.2017, 1, 5; Leyendecker/Mascolo, Fidans Liste, SZ 01./02.04.2017, 8; Regeln für Moscheevereine, SZ 03.04.2017, 6; Ramelsberger, Strafanzeige wegen türkischer Spionage, SZ 04.04.2017, 6; De Maizière erteilt Islamgesetz eine Absage, SZ 05.04.2017, 1; Imame scheitern mit Klage, SZ 08./09.04.2017, 6; Mächtiger Geheimdienst, Der Spiegel 14/2017, 24; Kazim, Erdoğans weltweites Spitzelnetz, Der Spiegel 14/2017, 76 f.; Kampf/Spinrath, Zehn Beschuldigte verschwunden, www.tagesschau.de 01.05.2017; Berlin finanziert Ditib wieder, SZ 02.05.2017, 6; BBA-Laudatio: https://bigbrotherawards.de/2017/politik-ditib).

BigBrotherAwards 2017 Ein Rückblick von Frans Jozef Valenta

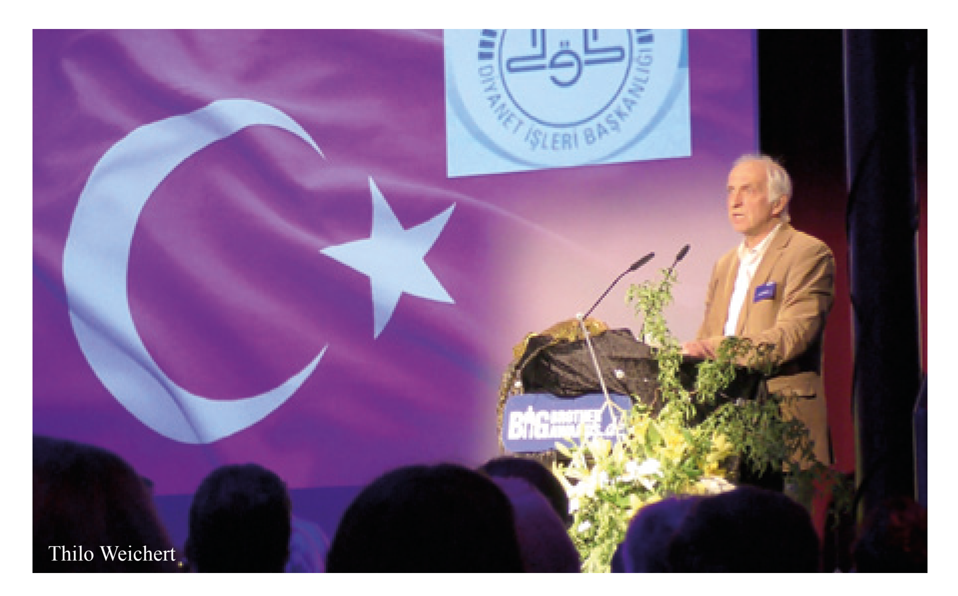

Peter Wedde



Rena Tangens

Die Eröffnungsrede hielt Peter Wedde über die Firma PLT – Planung für Logistik & Transport GmbH. Sie erhielt den BigBrotherAward 2017 in der Kategorie Arbeit für ihren PLT Personal-Tracker. Dieses Gerät zeigt Arbeitgebern in Echtzeit, wo sich Zeitungsausträger oder Paketzusteller befinden und wie schnell sie sich bewegen. Diese Totalkontrolle ist menschenunwürdig und sinnlos.

Rena Tangens erlärte in ihrer Rede, warum der deutsche IT-Branchenverband Bitkom den BigBrotherAward 2017 in der Kategorie Wirtschaft erhielt: Für sein unkritisches Promoten von Big Data, seine penetrante Lobbyarbeit gegen Datenschutz und weil er de facto eine Tarnorganisation großer US-Konzerne ist. Bitkom propagiert „Datenreichtum“ statt Datensparsamkeit – freie Bahn für Big Data Geschäftsmodelle. 8 Prozent der rund 1.600 Bitkom-Mitglieder kommen aus den USA. Mit dabei sind Amazon, Apple, Cisco, Ebay, Facebook, Google, Hewlett Packard, IBM, Intel, Paypal, Xerox und Microsoft. Bitkom ist inzwischen eine Lobbyorganisation von US-Konzernen, die unter falscher Flagge segeln.



Thilo Weichert


Pit Clausen

Die türkisch-islamische Union DİTİB erhält den BigBrotherAward 2017 in der Kategorie Politik dafür, dass bei der DİTİB tätige Imame für türkische Behörden und für den Geheimdienst MİT ihre Mitglieder und Besucher ausspioniert und sie so der Verfolgung durch türkisch-staatliche Stellen ausgeliefert haben sollen. Thilo Weichert erläuterte die besondere Bedeutung dieses Awards, denn er richtet sich diesmal nicht gegen eine Datenkrake, hier geht es um handfestes Bespitzeln, um das Ausnutzen menschlicher Kontakte von Angesicht zu Angesicht.

Der Oberbürgermeister von Bielefeld, Pit Clausen, zögerte zunächst, der Einladung von digitalcourage zu folgen und fragte sich, ob er wohl Teil einer Preisvergabe sei. Er würdigte die Bedeutung der BigBrotherAwards als Institution, die „immer öfter“ Reaktionen bewirkt.


Frank Rosengart

Die Technische Universität München und die Ludwig-Maximilian-Universität München erhielten den BigBrotherAward 2017 in der Kategorie Bildung für die Kooperation mit dem Online-Kurs-Anbieter Coursera. Coursera als Wirtschaftsunternehmen verfügt mit den Daten über den Lernerfolg der Studierenden über einen großen Datenschatz und behält sich vor, diesen auch wirtschaftlich zu nutzen. Frank Rosengart gab Einblicke in die Details dieses Geschäftsmodells, bei der die Datenschutz-Problematik ausgeblendet zu sein scheint.


Rolf Gössner

Die Bundeswehr und die Bundesministerin für Verteidigung erhielten den BigBrotherAward 2017 in der Kategorie Behörden für die massive digitale Aufrüstung der Bundeswehr mit dem neuen „Kommando Cyber- und Informationsraum“ (KdoCIR). Rolf Gössner erläuterte, wie diese digitale Kampftruppe mit (geplant) fast 14.000 Dienstkräften die Bundeswehr für den Cyberkrieg fit machen will – auch für militärische Cyberangriffe auf IT-Systeme und kritische Infrastrukturen anderer Staaten. Mit dieser Militarisierung des Internets beteiligt sich die Bundesrepublik am globalen Cyber-Wettrüsten durch Trojaner, Viren etc. – mit hohem Mißbrauchspotenzial ohne Parlamentsbeteiligung, ohne demokratische Kontrolle und ohne rechtliche Grundlage.


Andreas Liebold
Kerstin Demuth

Der Moderator Andreas Liebold befragte Kerstin Demuth zum Thema „Tadelnde Erwähnungen“. Hier gab es Berichte zum Ungang mit Facebook bei den öffentlich rechtlichen Medien, zu unberechtigten Ausweiskopien, zu BlaBlaCar, Immobilienscout 24, zum Bundesnachrichtendienst (BND), zur Europäischen Kommission im Zusammenhang mit geplanten Verboten anonymer Bezahlungen im Internet, zu WhatsApp und zu WordPress / Google Fonts.


padeluun

padeluun widmete seine Laudatio der Firma Prudsys AG. Sie erhielt den BigBrotherAward 2017 in der Kategorie Verbraucherschutz, weil sie Software anbietet, die Preisdiskriminierung erlaubt. Diese Software legt einen Preis fest, je nachdem, was sie über den jeweiligen Kunden herausfinden kann. Damit zählt nicht mehr, was ein Produkt kostet oder wert ist. So kommt es, dass zwei Menschen unterschiedliche Preise für die gleiche Ware bezahlen müssen. Die Händlerin oder der Händler müssen genug über uns wissen, um herauszufinden, welchen größtmöglichen Preis wir zu zahlen bereit sind. Im Marketing-Jargon heißt das: „Preisakzeptanzschwellen explorativ dynamisch austesten“. Der Händler weiß alles über seine Kunden, die Kunden nichts über die Händler.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

BKA-Gesetzes-Novelle mit Fußfessel verabschiedet

Der Bundestag beschloss am 27.04.2017 mit den Stimmen der Großen Koalition die Reform von Befugnissen des Bundeskriminalamtes (BKA). Darin ist u. a. vorgesehen, dass die Polizei künftig potenzielle Terroristen, sog. „Gefährder", unter Hausarrest stellen und ihren Aufenthalt elektronisch überwachen darf. Linke und Grüne lehnten die Gesetzesnovelle ab, mit der eigentlich Vorgaben des Bundesverfassungsgerichts (BVerfG) umgesetzt werden sollen. Dieses hatte eine frühere Novelle des BKA-Gesetzes vor einem Jahr teilweise für verfassungswidrig erklärt (BVerfG U. v. 20.04.2016, 1 BvR 966/09, 1 BvR 1140/09). Einzelne Bestimmungen waren stark unverhältnismäßig, die Lizenz zum großen Lauschangriff auch auf Kontakt- und Begleitpersonen von Verdächtigen war absolut verfassungswidrig.

In der Debatte vor der Gesetzesverabschiedung rühmte sich Bundesinnenminister Thomas de Maizière, an diesem Tage werde „Großes für die Sicherheit der Bürger", und das beinahe „im Stundenrhythmus", beschlossen. Es sei deshalb „ein guter Tag für die Sicherheit und ein guter Tag für Deutschland".

Gefährder ist gemäß dem neuen Gesetz eine Person, bei der es „Anhaltspunkte" dafür gibt, dass sie eine Straftat im Bereich des internationalen Terrorismus begehen könnte oder deren „individuelles Verhalten" es wahrscheinlich macht, dass eine solche Straftat geplant wird. Widersetzt sich ein Gefährder dem Hausarrest, droht ihm eine Haftstrafe von bis zu drei Jahren. Bei kleineren Verstößen wie bei Versuchen, die Fußfessel zu manipulieren, sollen Geldstrafen verhängt werden.

Der Bundesrat hatte befürchtet, dass die Länder größtenteils auf den nicht näher bezifferten Kosten für die Gefährderüberwachung sitzenbleiben dürften. Er forderte daher eine Art Übernahmegarantie der benötigten Geldmittel. Die Bundesregierung lehnte dies ab. Momentan tragen deutschlandweit rund 90 Personen eine Fußfessel von 3M und werden zentral von Bad Vilbel aus im Namen der Länderpolizeien überwacht. Nach ersten BKA-Schätzungen könnten nun zunächst 130 „hochaktive Personen" aus der Gefährderszene dazukommen.

Die Länderkammer sorgte sich u. a. auch, ob die vorgesehenen Regeln zum Datenschutz bei der Informationsübermittlung vor allem im internationalen Bereich den Maßstäben aus Karlsruhe genügen. Die Konferenz der Datenschutzbehörden des Bundes und der Länder hatte zuvor gegen den Regierungsvorschlag gravierende Bedenken vorgebracht. Die DatenschützerInnen monierten, dass „wichtige Datenschutzregeln und Verfahrenssicherungen" im gesamten Polizeirecht zurückgenommen würden. Das Vorhaben der Bundesregierung beschränke sich aber nicht darauf, die Vorgaben des Verfassungsgerichts oder weitere Regeln der EU umzusetzen. Vielmehr werde das polizeiliche Datenschutzrecht grundlegend verändert und auf den Kopf gestellt, was sich zudem auch auf Polizeibehörden der Länder auswirke.

So wird der Informationsverbund für die Polizei des Bundes und der Länder völlig neu gefasst. Dieser ist dann nicht mehr nach einzelnen Dateien untergliedert, was, so die Datenschutzbeauftragten, „zu unverhältnismäßig weitreichenden Speicherungen" führt. Zudem erklärt der Entwurf Dateierrichtungsanordnungen für verzichtbar, die bisher erforderlich sind, um Datenbanken wie die Anti-Terror- oder die Hooligan-Datei erstellen zu dürfen. Dieses Instrument war bislang „Ausgangspunkt sowohl für datenschutzrechtliche Kontrollen als auch die Selbstkontrolle der Polizeibehörden". In den Anordnungen werde im Einklang mit der Verfassung festgelegt, „zu welchen Zwecken personenbezogene Daten gespeichert sind".

Das Gesetz erlaubt es, Informationen zu allen erfassten Personen „themenübergreifend" zu verknüpfen und miteinander abzugleichen. Zugleich verkürzt er die Kontrollmöglichkeiten der Datenschutzbeauftragten. Künftig dürfen alte Informationsbestände auch zu lediglich Verdächtigen „bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden". Dafür soll es schon genügen, wenn die betroffene Person als Zeuge oder Kontaktperson erneut auffällig wird. Auch dies verstößt nach Ansicht der DatenschützerInnen „gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot".

Die vorgesehene Reform hatten auch andere ExpertInnen in einer Anhörung im Bundestag am 20.03.2017 kritisiert. Der Mainzer Staatsrechtler Matthias Bäcker befürchtete, dass der Entwurf und die darin skizzierte „fundamentale Umgestaltung" des BKAs entweder in Karlsruhe scheitere oder von Verwaltungsgerichten stark eingeschränkt werde. Ulf Buermeyer, Richter am Landgericht Berlin, gab zu bedenken, dass die Grundsätze der Datensparsamkeit und der Zweckbindung in ihr Gegenteil verkehrt würden. Der „Terrorismusteil" des Gesetzes wäge nicht hinreichend zwischen Freiheit und Sicherheit ab, sondern schramme „konsequent an der rechten Leitplanke entlang". Besonders augenfällig werde dies etwa bei den Befugnissen für den Einsatz von Staatstrojanern.

Auf weniger Kritik war elektronische Fußfessel für terroristische „Gefährder" gestoßen. Der Würzburger Staatsrecht-

ler Kyrill-Alexander Schwarz bezeichnete eine solche Aufenthaltsüberwachung als „einen Akt experimenteller Gesetzgebung“. Natürlich werde diese Maßnahme „einen zu allem Entschlossenen“ nicht davon abhalten können, Anschlagspläne in die Tat umzusetzen. Sie sei aber milder als etwa ein auch denkbarer „Präventivgewahrsam“. Der Bonner Rechtswissenschaftler Klaus Ferdinand Gärditz sprach von einem „sinnvollen Kompromiss“, mit dem sich zumindest die Vorbereitung von Terrorattacken erheblich erschweren lasse.

Schwarz-Rot besserte mit einem Änderungsantrag parlamentarisch trotz der teilweise vorgetragenen Fundamentalkritik fast nur noch „redaktionelle Versehen“ aus, sodass nun etwa Löschfristen zumindest wieder greifen. Zudem stellten die Regierungsfraktionen klar, dass das BKA auch „Altdaten“ für eine Übergangsfrist bis Mai 2018 weiterverwenden darf, ohne diese einzeln neu kennzeichnen zu müssen. Generell will der Gesetzgeber nach den Vorgaben des Verfassungsgerichts etwa die Lizenzen zum großen Lauschangriff etwas beschränken oder die Voraussetzungen für den Einsatz von Bundestrojanern deutlicher fassen.

Die Bundesdatenschutzbeauftragte Andrea Voßhoff sieht mit dem Gesetzesbeschluss die Zweckbindung bei der Polizei und damit einen „Grundpfeiler des deutschen Datenschutzrechts“ gefährdet. Informationen zu Drogendelikten, die bisher zum Beispiel in der Falldatei Rauschgift gespeichert wurden, können künftig mit anderen Daten verknüpft und ausgewertet werden. Dies sei etwa im Zusammenhang mit Steuerstraftaten oder bei Polizeikontrollen im Umfeld von Demonstrationen der Fall und angesichts der technischen Entwicklung problematisch.

Am gleichen Tag beschloss der Bundestag auch ein Gesetz zum besseren Schutz „von Vollstreckungsbeamten und Rettungskräften“, wonach künftig Attacken gegen diese schon bei „allgemeinen Diensthandlungen“ wie einer Streifenfahrt und nicht mehr nur bei Vollzugshandlungen wie einer Festnahme mit bis zu fünf Jahren Haft geahndet werden können. Beschlossen wurde zudem ein Gesetz zur Speicherung von Fluggastdaten (Krempl, BKA-Gesetz: Bundestag stimmt für E-Fußfessel für Gefährder und „Polizei-Cloud“, www.heise.de 27.04.2017; Krempl, Datenschützer lehnen geplante Novelle des BKA-Gesetzes als verfassungswidrig ab, www.heise.de 21.03.2017; Rossmann, Fesseln auf Verdacht, SZ 28.04.2017, 5).

Bund

Bundestag beschließt PNR-Gesetz zu Fluggastdaten

Der Bundestag beschloss mit den Stimmen der Großen Koalition und nur mit formalen Änderungen am 27.04.2017 ein Gesetz, das dem Staat erlaubt, von Mai 2018 an auch hierzulande Flugpassagierdaten fünf Jahre lang zu sammeln, automatisiert mit Sicherheitsdateien abzugleichen sowie anderweitig auszuwerten. Vorbilder hierfür sind die Praktiken in den USA oder Großbritannien.

Die Opposition stimmte geschlossen gegen das Vorhaben, mit dem eine EU-Richtlinie umgesetzt werden soll. Insgesamt werden künftig 60 Datenkategorien erfasst, darunter Essenswünsche, E-Mail- und andere Kontaktadressen sowie eventuelle Vielfliegernummern. Die Passenger Name Records (PNR) müssen zunächst sechs Monate „unmaskiert“, danach viereinhalb Jahre ohne direkten Personenbezug gespeichert werden. Gegebenenfalls sollen die Daten auch im zweiten Stadium „re-identifiziert“ werden können. Dazu kommen weitgehende Bestimmungen zum Informationsaustausch mit anderen Mitgliedsländern, Europol und Drittstaaten.

Von der Option, neben Flügen aus der EU hinaus auch innereuropäische Strecken zu erfassen, soll laut dem Beschluss Gebrauch gemacht werden. Als nationale PNR-Zentralstelle ist das Bundeskriminalamt (BKA) vorgesehen. Es soll die Informationen an andere Sicherheitsbehörden einschließlich der Geheimdienste weitergeben dürfen. Das Fluggastdaten-Informationssystem einzurichten wird laut offiziellen Schätzungen 78 Millionen Euro kosten. Dazu kommen sollen 65 Millionen Euro jährliche Betriebskosten. Die Luftfahrtunternehmen werden laut Regierungsangaben einmalig bis zu 3,96 Millionen Euro sowie zusätzlich jährlich zwischen 594.000 und 3,7 Millionen Euro aufwenden müssen.

Der Europäische Gerichtshof (EuGH) prüft parallel das PNR-Abkommen zwischen der EU und Kanada und dabei auch, ob diese Form der Vorratsdatenspeicherung grundsätzlich rechtmäßig ist. Das Gutachten soll bald vorliegen. CDU/CSU und SPD wollten trotz der Bitte der Datenschutzbeauftragten Andrea Voßhoff mit der Gesetzgebung nicht warten, um die Maßgaben der Luxemburger Richter noch zu berücksichtigen. Gegebenenfalls muss der Gesetzgeber also bald schon nachbessern (Krempl, Bundestag bringt Fluggastdatenspeicherung auf den Weg, www.heise.de 28.04.2017).

Bund

BAMF soll Handys von Flüchtlingen auslesen dürfen

Mitarbeiter des Bundesamtes für Migration und Flüchtlinge (BAMF) sollen gemäß einem Gesetzentwurf des Bundesinnenministeriums (BMI), über den die Presse berichtete, künftig die Mobiltelefone von Flüchtlingen überprüfen dürfen, um deren Identität und Herkunft festzustellen. Danach soll „zur besseren Durchsetzung der Ausreisepflicht“ die bisher nötige Einwilligung der Betroffenen künftig umgangen werden können. Bis zur Ressortabstimmung will das BMI keine weiteren Einzelheiten bekanntgeben.

Ausländerbehörden ist zwar seit der Novelle des Aufenthaltsrechts von 2015 der Zugriff auf Mobiltelefone und andere Datenträger im Prinzip erlaubt. Das BAMF war dabei aber bisher auf die Zustimmung der Asylsuchenden angewiesen. Ansonsten bedarf das Auslesen von Handys hierzulande normalerweise eines richterlichen Beschlusses und ist nur möglich, wenn der Verdacht auf eine Straftat vorliegt. Um die Herkunft eines Menschen festzustellen, hat das BAMF bisher mit Sprachgutachten und mit gezielten Nachfragen, zum Beispiel nach Staatsoberhäuptern des behaupteten Herkunftslandes oder touristischen

Attraktionen in der behaupteten Geburtsstadt, versucht, mehr Klarheit zu bekommen.

Gemäß den veröffentlichten Unterlagen soll die künftige Untersuchung von Mobiltelefonen und anderen Datenträgern in großem Umfang stattfinden können. Im Jahr 2016 habe man bei 50% bis 60% der Asylsuchenden ein solches Vorgehen in Betracht gezogen, also bei etwa 150.000 Menschen. Die Außenstellen des BAMF sollen mit forensischer Hard- und Software aufgerüstet werden, so dass täglich ca. 2.400 Datenträger ausgelesen werden können. Gemäß dem Ausländerzentralregister befanden sich Anfang 2017 213.000 „vollziehbar ausreisepflichtige Ausländer“ in Deutschland.

Mit dem Gesetz soll verhindert werden, dass Flüchtlinge bei Behörden verschiedene oder falsche Personalien angeben. Dies geschieht in manchen Fällen aus Angst vor drohender Abschiebung oder auch, um mehrfach Sozialleistungen zu kassieren. So hatte sich beispielsweise der Attentäter vom Berliner Breitscheidplatz, Anis Amri, hinter 14 verschiedenen Identitäten versteckt. Der Bundesrat hatte 2015 angemerkt, dass das Auslesen von Mobilgeräten für die Abschiebung problematisch sei, weil es den „unantastbaren Kernbereich persönlicher Lebensgestaltung“ verletzen könnte. Die Grenze zwischen Daten, die für die Identitätsfeststellung geeignet seien und Daten, die unter dem Schutz der Privatsphäre stünden, seien „fließend und nicht rechtssicher abgrenzbar“. Die Geodaten der Mobiltelefone und gespeicherte Kontakte sollen darüber Aufschluss geben, woher jemand stammt oder wo er oder sie sich zuletzt aufgehalten hat.

In einem ersten Gesetzentwurf vom Herbst 2016 wurde noch zwischen abgelehnten Asylbewerbern unterschieden, die ohne eigenes Verschulden nicht ausreisen können, beispielsweise wegen Krankheit oder aus familiären Gründen, und solchen, die durch Täuschung über ihre Identität ein Abschiebehindernis erzwingen. Von dieser Eingrenzung war in dem neuen Referentenentwurf keine Rede mehr.

Eine „vollständige Sicherung von Datenträgern von bereits länger in Deutschland aufhältigen Asylsuchenden“ werde zwar nicht angestrebt. Doch senkt der Gesetzentwurf auch die Hürden bei der Weitergabe von besonders geschützten Daten aus medizinischen Attesten.

In Nordrhein-Westfalen waren Februar 2017 220 Personen als Gefährder eingestuft, 41 davon sind in Deutschland lebende Menschen einer anderen Nationalität. Etwa jeder Vierte von ihnen war „vollziehbar“ zur Ausreise verpflichtet. Fünf von ihnen waren in Haft. Die anderen fünf waren ein Palästinenser, bei dem der Reiseausweis nicht zur Rückkehr berechtigt, ein Flüchtling, bei dem es ein Abschiebeverbot des BAMF gibt, sowie ein Tunesier, ein Marokkaner und ein Jordanier. Im Fall des Gefährders aus Jordanien läuft das sog. Passersatzverfahren schon seit siebeneinhalb Jahren (Kampf/Leyendecker, Das Handy als Pass-Ersatz, SZ 20.02.2017, 5; Kampf, Handys von Flüchtlingen im Visier, www.tagesschau.de 19.02.2017).

Bund

Automatisierter Zugriff der Geheimdienste auf Passbilder?

Die Bundesregierung will den Ämtern für Verfassungsschutz und dem Bundesnachrichtendienst (BND) den verdeckten Zugriff auf die digitalisierten Passbilder der Bundesbürger erlauben. Das sieht der Regierungsentwurf eines „Gesetzes zur Förderung des elektronischen Identitätsnachweises“ vor, der am 27.04.2017 im Bundestag zum zweiten Mal debattiert und anschließend verabschiedet werden sollte (BT-Drs. 18/11279 v. 22.02.2017). Ziel der Regelung ist es laut Bundesregierung, die Online-Ausweisfunktion des elektronischen Personalausweises leichter anwendbar und attraktiver zu machen. Der Entwurf sieht vor, dass jeder neue Personalausweis künftig mit einer einsatzbereiten Funktion zum elektronischen Identitätsnachweis ausgegeben wird. Unternehmen und Behörden sollen zudem leichter eine Berechtigung erhalten, um Online-Ausweisfunktionen anzubieten. In Fällen, in denen das persönliche Erscheinen bei Behörden oder Banken unumgänglich ist, soll dort der Personalausweis künftig auch eingesetzt werden, um das Verfahren zu beschleunigen.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Andrea Voßhoff (CDU), hatte in einer Expertenanhörung kritisiert, durch die geplanten Zugriffsrechte entstehe ein „nahezu voraussetzungsloser Abruf des Lichtbildes“ durch Polizei und Nachrichtendienste. Aufgrund der von verschiedenen Seiten geäußerten Bedenken haben Union und SPD den Punkt kurzfristig von der Tagesordnung genommen. So meinte der SPD-Innenpolitiker Mahmut Özdemir: „Wir haben Redebedarf“. Schon bislang können Sicherheitsbehörden auf Passbilder zugreifen, ohne dass Pass- oder Meldeämter etwas merken, wenn es um Strafverfolgung geht. Nach dem Entwurf soll dies auch zur Gefahrenabwehr und generell für alle Geheimdienste möglich werden. So soll verhindert werden, dass Betroffene mitbekommen, wenn sie ins Visier geraten.

Schon seit November 2005 werden die PassantragstellerInnen gebeten, einen möglichst „neutralen“ Gesichtsausdruck beim Erstellen ihrer Passfotos zu wählen, um eine möglichst zuverlässige biometrische Zuordnung vornehmen zu können und Bilder verfügbar zu haben, die notfalls für Fahndungen genutzt werden können. Inzwischen wird das Bild auch digital abgespeichert. Seit 2007 dürfen Polizei und Ordnungsbehörden automatisiert auf die Bildbestände zugreifen, ohne eine Begründung angeben zu müssen, eine Möglichkeit die nun auch zur Gefahrenabwehr sowie den Verfassungsschutzbehörden, dem BND und dem Militärischen Abschirmdienst eingeräumt werden soll (Passbild u. Passbilder für Geheimdienste, SZ 27.04.2017, 4 u. 6).

Bundesweit

Antifolterstelle kritisiert Haftzustände

Die regierungsunabhängige „Nationale Stelle zur Verhütung von Folter“ hat menschenunwürdige Zustände in einigen deutschen Haftanstalten festgestellt. Nach Besuchen von Gefängnissen und Polizeiwachen kritisierte sie, dass die Intimsphäre von Gefangenen oft nicht

ausreichend geschützt sei. So seien etwa Einzelzellen mit zwei Gefangenen belegt, ohne dass die Toilette abgetrennt sei. Dies verletze die Menschenwürde.

Die Stelle wurde auf Basis der Antifolterkonvention der Vereinten Nationen 2009 geschaffen, um die Wahrung der menschenwürdigen Unterbringung und Behandlung im Freiheitsentzug sicherzustellen. Es gibt in Deutschland etwa 13.000 Einrichtungen, in denen Menschen in irgendeiner Form die Freiheit entzogen wird, von Justizvollzugsanstalten (JVA) über Jugendhilfeeinrichtungen bis hin zu Pflegeheimen, wo Senioren mitunter fixiert werden. In ihrem aktuellen Bericht für das Jahr 2016, in dem etwa 70 Häuser besucht wurden, bemängelt die Menschenrechtsorganisation, dass in Haftzellen einiger Gefängnisse und Polizeistationen selbst der Toilettenbereich videoüberwacht sei. Erwähnt werden Frauengefängnisse in Brandenburg, Nordrhein-Westfalen, Hamburg und Bremen. Die Aufnahmen liefen in Sicherheitszentralen auf, in denen auch Männer vor den Monitoren säßen. Dass eine Überwachung auch menschenwürdig möglich sei, zeige vorbildlich etwa die JVA in Rohrbach in Rheinland-Pfalz. Dort werde der Toilettenbereich nur verpixelt dargestellt. Kritisch gesehen wird auch, wenn sich Gefangene vollständig entkleiden müssen, um durchsucht zu werden. Dies sei ein „schwerwiegender Eingriff“ in die Persönlichkeitsrechte und dürfe nicht zur Routine werden (Kastner, Videokamera auf der Toilette, SZ 21.05.2017, 6).

Bayern

Fußfessel für Stalker?

Bayerns Justizminister Winfried Bausback (CSU) will Stalkern künftig elektronische Fußfesseln anlegen lassen. Damit sollten Opfer vor Wiederholungstätern besser geschützt werden: „Stalking heißt: Die Täter nehmen den Opfern die Möglichkeit, ihr normales Leben, einen normalen Alltag zu leben. Deshalb fordere ich die elektronische Fußfessel für verurteilte Stalker, von denen weiterhin Stalking-Gefahr ausgeht.“ Dasselbe gelte für Menschen, die wiederholt und schwer gegen gerichtliche Kontaktverbote nach dem Gewaltschutzgesetz verstoßen. Das Thema soll Gegenstand der Justizministerkonferenz werden. Rund 22 000 Fälle werden demnach pro Jahr in Deutschland angezeigt (Fußfessel für Stalker, SZ 02.05.2017, 6).

Niedersachsen

Datenschutzbeauftragte beanstandet polizeilichen Bodycam-Pilotversuch

Barbara Thiel, die Landesbeauftragte für den Datenschutz in Niedersachsen, bewertet den seit Dezember 2016 stattfindenden Pilotversuch der niedersächsischen Polizei mit Bodycams als rechtswidrig. Dem Einsatz der Kameras, die Polizisten auf ihren Schultern tragen, fehle die Rechtsgrundlage. Thiel beanstandete den Pilotversuch förmlich. Das Innenministerium hatte keine so genannte Vorabkontrolle erstellt und den Piloten trotz Aufforderung nicht beendet. Die Vorabkontrolle dient der Prüfung, ob die Datenverarbeitung angemessen und sicher ist, und wird nach dem Niedersächsischen Datenschutzgesetz zwingend vorgeschrieben. Sie muss vorgenommen werden, bevor eine neue Technik eingeführt wird.

Der Stellvertreter von Thiel, Christoph Lahmann, erläuterte: „Eine ausdrückliche Befugnisnorm ist zwingend erforderlich, um die Anfertigung von Bildaufnahmen und damit den Eingriff in das Grundrecht auf informationelle Selbstbestimmung zu rechtfertigen“. Körperkameras griffen verglichen mit anderen Formen der Videoüberwachung besonders schwerwiegend in die Grundrechte ein, da die Kameras direkt in Gesichtshöhe die Betroffenen erfassten und regelmäßig unbeteiligte Dritte aufgenommen würden. Lahmann: „Wir sind nicht grundsätzlich gegen Bodycams bei der Polizei – die Kameras dürfen aber nicht an Recht und Gesetz vorbei betrieben werden“. Der niedersächsische Landtag berät einen Gesetzentwurf der Landesregierung zur Überarbeitung des niedersächsischen Polizeigesetzes, der eine Regelung für Körperkameras vorsieht. Wenn diese Neuregelung beschlossen werde und in Kraft getreten sei, dürften die Bodycams eingesetzt werden.

In anderen Bundesländern laufen ebenso Pilotversuche mit Bodycams, die Polizisten vor allem zu ihrem eigenen Schutz tragen. In Rheinland-Pfalz kritisierte der dortige Beauftragte Dieter Kugelmann, dass dabei neben Bildern „auch Sprache“ aufgezeichnet werde. Die Rechtsgrundlagen erlaubten Tonaufnahmen zwar grundsätzlich, er halte diese Praxis aber für sehr bedenklich. In Hamburg wurde für die Bodycams das Gesetz über die Datenverarbeitung der Polizei (PolDVG) geändert. Danach ist der Einsatz „technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen“ für „Maßnahmen zur Gefahrenabwehr oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten in öffentlich zugänglichen Bereichen“ zulässig (Wilkens, Datenschutzbeauftragte: Niedersächsische Polizei testet Bodycams rechtswidrig, www.heise.de 08.01.2017).

Datenschutznachrichten aus dem Ausland

UN-Sonderberichterstatter: Massenüberwachung nicht effektiv

In einem Bericht vom 24.02.2017 kommt der UN-Sonderberichterstatter für das Recht auf Privatsphäre, Joseph Cannataci, zu dem Schluss, dass die umfassenden Überwachungsmaßnahmen, die in Deutschland, Frankreich, Großbritannien und den USA eingeführt wurden, weder effektiv noch verhältnismäßig sind. Er warnt davor, große Datensammlungen anzulegen, die in den Händen einer schlechten Regierung zu

einer Waffe gegen die eigene Bevölkerung werden können. Man dürfe in der Sicherheitspolitik jetzt „nicht die Angstkarte spielen“. Stattdessen plädiert er für wirksame Maßnahmen, die nicht unverhältnismäßig in die Privatsphäre aller Menschen eingreifen und erinnert daran, dass das Recht auf Privatsphäre universell ist.

Der Bericht des UN-Sonderberichterstatters für das Recht auf Privatsphäre: https://www.documentcloud.org/documents/3514983-UN-special-rapporteur-on-the-right-to-privacy.html

EU

110 Mio. € Strafe gegen Facebook wegen Falschangaben zum Datenmanagement

Die EU-Kommission teilte am 18.05.2017 mit, dass sie gegen Facebook 110 Millionen Euro Strafe verhängt, weil das US-Unternehmen bei der Übernahme von WhatsApp irreführende Angaben gemacht hat. Facebook hat nach Angaben der Kommission bei der Anmeldung der Übernahme des Messenger-Dienstes im Jahr 2014 erklärt, dass es nicht zuverlässig möglich sein werde, einen automatischen Datenabgleich zwischen den Benutzerkonten beider Dienste einzurichten. Im August 2016 hatte Facebook dann jedoch angekündigt, künftig die Telefonnummern von WhatsApp-Nutzenden mit Facebook-Profilen zu verknüpfen. Wegen der damit verbundenen Täuschung erfolgte nun die Sanktion. Die Höhe der Geldbuße begründete Wettbewerbskommissarin Margrethe Vestager mit der abschreckenden Wirkung für falsche Angaben bei Verfahren zur Fusionskontrolle: „Die Kommission hat festgestellt, dass ein automatischer Abgleich der Facebook- und der WhatsApp-Nutzerprofile – entgegen den von Facebook im Rahmen des Fusionskontrollverfahrens von 2014 gemachten Angaben – bereits im Jahr 2014 technisch möglich war, und dass den Facebook-Mitarbeitern diese Möglichkeit bekannt war. Die Kommission muss sich beim Erlass ihrer Beschlüsse über die Auswirkungen von Zusammenschlüssen auf den Wettbewerb auf umfassende und präzise Informationen stützen können.“

Facebook betonte dagegen: „Wir haben seit den allerersten Kontakten zur Kommission nach bestem Wissen und Gewissen gehandelt und versucht, zu jeder Zeit korrekte Informationen zu liefern.“ Die Fehler in den Papieren von 2014 seien keine Absicht gewesen. Zudem habe die Kommission bestätigt, dass sie für das Ergebnis des Genehmigungsverfahrens nicht entscheidend gewesen seien. Tatsächlich erklärte Vestagers Behörde, Facebooks unrichtige Angaben seien zwar relevant, aber nicht ausschlaggebend gewesen. Die Kommission habe schon damals auch das hypothetische Szenario durchgespielt, dass ein Nutzerabgleich möglich wäre. Der jetzige Beschluss habe deshalb keine Auswirkungen auf die 2014 erteilte Genehmigung.

Facebook hatte im Februar 2014 für WhatsApp 19 Mrd. US-Dollar ausgegeben. Im Kaufpreis inbegriffen waren nicht nur die Marke und die Chat-Software, sondern auch Hunderte Millionen Telefonnummern, die mit WhatsApp verknüpft sind. Schon damals befürchteten DatenschützerInnen, dass Facebook die neuen Daten mit den vorhandenen Informationen bei Facebook verbindet (DANA 2/2014, 82). WhatsApp hatte sich damals eindeutig festgelegt: „Und das wird sich für euch, unsere Benutzer, ändern: Nichts.“ Zwar gab es kleine Verbesserungen bei dem Dienst, z. B. wurde eine Ende-zu-Ende-Verschlüsselung eingeführt. Doch September 2016 änderte WhatsApp die Nutzungsbedingungen und erlaubte, dass Telefonnummern an Facebook übertragen werden können, verbunden mit Informationen, wann und wie häufig eine NutzerIn die App verwendet. Zweck des Abgleichs sollte es sein, die Werbung auf Facebook zu verbessern, also dafür zu sorgen, dass Werbung noch besser personalisiert werden kann.

Damals kritisierte Klaus Müller vom Verbraucherzentrale Bundesverband: „Verbraucher vertrauten darauf, dass ihre Daten allein bei WhatsApp bleiben und kein Datentransfer zu Facebook erfolgt. Ihr Vertrauen wurde enttäuscht“ (DANA 4/2016, 192). Der Hamburgische Datenschutzbeauftragte Johannes Caspar verbot die Weitergabe der Handynummern (DANA 4/2016, 194 f.). Facebook wehrte sich vor Gericht und verlor vorläufig Ende April 2017, so dass deutsche Nutzende zunächst vor dem Datenaustausch geschützt sind. Doch hat das Unternehmen angekündigt, in Berufung zu gehen. Caspar begrüßte die Strafe der EU-Kommission: „Die Luft in der EU wird zusehends dünner für Unternehmen, die den Vorgaben des Datenschutzrechts nicht entsprechen. Unternehmen, die dies nicht erkennen, werden insbesondere auf dem EU-Markt keinen Erfolg haben. Zuletzt häuften sich Strafen gegen Facebook: Italienische Behörden verhängten eine Woche vor Brüssel eine Geldbuße von 3 Mio. Euro wegen der Datenweitergabe von WhatsApp an Facebook. In Frankreich wurde eine Strafe von 150.000 Euro gegen Facebook ausgesprochen wegen mangelndem Schutz der Nutzenden vor Werbetreibenden.

Die Geldbuße hätte mehr als doppelt so hoch ausfallen können. Die maximale Strafe in solchen Fällen ist ein Prozent des Jahresumsatzes. Strafmildernd wirkte, dass Facebook kooperierte und die falschen Angaben einräumte. Der Europaabgeordnete Markus Ferber (CSU) kritisierte die Strafhöhe. Der Vorgang zeige, mit welcher Naivität die Kommission an wettbewerbsrechtliche Fragen der Digitalwirtschaft herangehe: „Vor allem auf kartellrechtliche Kennzahlen wie Umsatz und Gewinn zu schauen und die wichtige Rolle, die Daten für Unternehmen der Digitalwirtschaft spielen, zu ignorieren, wird der Komplexität des Problems nicht gerecht. Der FDP-Abgeordnete Mihael Theurer forderte, dass „wir dringend neue kartellrechtliche Regeln benötigen, die sich nicht nur zuvörderst am Umsatz orientieren“.

Auch das Bundeskartellamt in Bonn prüft, ob Facebook seine Marktmacht missbraucht, indem es Daten zusammenträgt, ohne die Nutzenden darüber genau zu informieren. Dessen Chef Andreas Mundt kritisierte immer wieder, dass das bisherige Wettbewerbsrecht für die Digitalbranche nicht ausreiche.

In den USA gab es schon unter Präsident Barack Obama scharfe Kritik am wettbewerbsrechtlichen Vorgehen von Brüssel. So waren den US-Behörden die Ermittlungen gegen die Steuertricks

von Apple ein Dorn im Auge, die 2016 zu einer verhängten Strafe in Höhe von 13 Mrd. Euro führten. In einem Papier des US-Finanzministeriums vom August 2016 wurde der Kommission vorgeworfen, sich wie eine supranationale Steuerbehörde" aufzuspielen. Wegen unerlaubter Rabatte wurde 2009 gegen Intel eine Zahlung von 1,06 Mrd. Euro verhängt. Microsoft erhielt 2013 wegen seines Browserzwangs eine Strafe von 561 Mio. Euro, 2008 wegen zu hoher Lizenzgebühren eine Strafe von 899 Mio. Euro (WhatsApp-Übernahme: EU verlangt 110 Millionen Euro Strafe von Facebook, www.heise.de 18.05.2017; Mühlauer, EU-Kommission bestraft Facebook, SZ 19.05.2017, 1, Mühlauer/Strathmann, Sie schlägt wieder zu, SZ 19.05.2017, 17).

EU

Kommission führt Whistleblowing-System ein

Wer brisante Informationen über geheime Kartelle oder Verstöße gegen das Wettbewerbsrecht hat, kann Hinweise dazu jetzt der EU-Kommission anonym online zukommen lassen. Das neue Instrument soll auch abschreckend wirken.

Die Kommission erhofft sich von dem E-Mail-Kommunikationsangebot mehr Hinweise auf Kartellrechtsverletzungen. Die für Wettbewerbspolitik zuständige EU-Kommissarin Margrethe Vestager sagte: „Wem Geschäftspraktiken falsch erscheinen, der kann nun selbst dazu beitragen, solche Missstände zu beseitigen." Insiderwissen könne ein wirksames Mittel sein, „um die Kommission beim Aufdecken von Kartellen und anderen wettbewerbswidrigen Praktiken zu unterstützen". Solche Informationen könnten helfen, „dass wir mit unseren Ermittlungen rasch und effizient ans Ziel kommen".

Das System soll es erleichtern, dass Wettbewerbswidrigkeiten aufgedeckt werden, die der europäischen Wirtschaft schweren Schaden zufügen könnten. Dazu zählt die Kommission Absprachen bei Preisen oder bei Angeboten in Ausschreibungen, „das Zurückhalten von Produkten vom Markt" oder den ungerechtfertigten Ausschluss von Wettbewerbern. Bisher seien die meisten Kartelle über ein spezielles Kronzeugenprogramm aufgedeckt worden. Nun werde es auch für nicht direkt an einem Komplott beteiligte Einzelpersonen einfacher, die Kommission auf die richtige Spur zu bringen.

Der E-Maildienst ist ein speziell verschlüsseltes Mitteilungssystem über den externen Dienst secway.info, das eine wechselseitige Kommunikation ermöglicht. Antworten können über ein Passwort abgerufen werden. Übermittelt werden ausschließlich die Inhalte der Nachrichten. Metadaten, die Rückschlüsse auf die Identität des Absenders zulassen könnten, bleiben außen vor. Die Technik wird der Kommission zufolge auch bereits in Behörden in Deutschland, Dänemark und anderen Mitgliedsstaaten eingesetzt. Eine allgemeine anonyme Mailbox für Whistleblower betreibt die Behörde noch nicht. Der EU-Datenschutzbeauftragte Giovanni Buttarelli hatte voriges Jahr die Verwaltung aufgefordert, „sichere Kanäle" für Hinweisgeber einzurichten (Krempl, Kartellrecht: EU-Kommission ermuntert zu anonymem Whistleblowing, www.heise.de 17.03.2017).

Italien

Millionenstrafe gegen WhatsApp wegen Verbrauchertäuschung

Die italienische Wettbewerbsbehörde hat gegen WhatsApp ein Bußgeld in Höhe von drei Millionen Euro wegen irreführenden Behauptungen gegenüber den Nutzenden verhängt. Diese seien in dem Glauben gelassen worden, den Kurzmitteilungsdienst nicht mehr nutzen zu können, sollten sie den neuen Nutzungsbedingungen und insbesondere der Weitergabe der persönlichen Daten an die Konzernmutter Facebook nicht komplett zustimmen. Es sei möglich gewesen, den Nutzungsbedingungen auch teilweise zuzustimmen und die Weitergabe der Daten aus dem WhatsApp-Account abzulehnen. Mit der Irreführung der Nutzer habe WhatsApp gegen die Vorschriften im Verbraucherkodex verstoßen, erklärte die Behörde (WhatsApp muss Strafe in Italien zahlen, www.heise.de 13.05.2017).

Großbritannien

1,6 Mio. PatientInnendaten des NHS für Deep Mind

Die sog. „künstliche Intelligenz" (KI) erforschende Google-Tochtergesellschaft Deep Mind arbeitet schon längere Zeit mit dem staatlichen britischen National Health Service (NHS) zusammen. Die KI-Fachleute haben eine App entwickelt namens Streams, die Ärzte und Krankenpfleger nach einer Testphase mittlerweile in mehreren Krankenhäusern in London in der alltäglichen Behandlung ausprobieren.

Die App soll den MedizinerInnen dabei helfen herauszufinden, ob eine PatientIn für akutes Nierenversagen anfällig ist. Im Zusammenhang damit sterben gemäß Angaben des NHS jedes Jahr 40.000 Menschen in Großbritannien. Die NHS-Fachleute schätzen, dass ungefähr ein Viertel davon durch Vorbeugung verhindert werden kann. Sowohl die Krankenhausgruppe Royal Free als auch Deep Mind-Mitgründer Demis Hassabis teilten über den Kurznachrichtendienst Twitter mit, dass die Rückmeldungen aus der Medizin positiv seien.

Streitig ist, ob die Kooperation zwischen der Google-Tochtergesellschaft und dem NHS rechtlich einwandfrei ist. Um der Medizin-App das Diagnostizieren beizubringen, hat die britische Gesundheitsbehörde den Deep-Mind-Forschenden nämlich die Daten von 1,6 Millionen PatientInnen zur Verfügung gestellt, die den entsprechenden Personen zugeordnet werden können. Die ranghöchste Datenschutzbeauftragte im britischen Gesundheitsministerium teilte dem Chef des NHS-Krankenhauses Royal Free ihre Bewertung mit, dass die Bereitstellung der Patientendaten durch den NHS an Deep Mind auf einer „unangemessenen rechtlichen Grundlage" erfolgt sei. Die Meinung ist relevant, sie fließt in die offizielle Untersuchung dieses Vorgangs durch die britische Datenschutzbehörde IOC ein, die sich dem Bericht zufolge „kurz vor dem Abschluss" befindet.

Konkret dreht sich die rechtliche Debatte darum, ob Deep Mind von jedem einzelnen der 1,6 Millionen PatientIn-

nen eine persönliche Einverständniserklärung hätte einholen müssen. Nach britischem Recht ist es offenbar legal, dies auszulassen, wenn die Daten für die direkte medizinische Behandlung verwendet werden. Auf diesem Standpunkt stehen die Fachleute von Deep Mind. Die Gesundheits-Datenschützerin argumentiert hingegen, dass die Daten von Deep Mind eben nicht zur direkten PatientInnen-Behandlung verwendet worden seien, sondern, um besagte Medizin-App zu „trainieren" und für den NHS zu entwickeln.

In einer Stellungnahme zu dem Sachverhalt teilte der Klinikbetreiber Royal Free mit, dass dieses Projekt „eines der ersten seiner Art innerhalb des NHS" sei und es „immer Lektionen gibt, die wir aus Pionierarbeit lernen können". Ein Sprecher von Deep Mind erklärte, dass die Daten „niemals für kommerzielle Zwecke verwendet worden oder mit Google-Produkten, Diensten oder Werbung kombiniert worden sind – und es niemals werden". Die Diskussion über Gesundheitsdaten gewann in Großbritannien große Aufmerksamkeit auch wegen der eine Woche zuvor erfolgenden Cyberattacke durch den Wurm „Wannacry", durch die mehr als 220.000 Computer in 150 Ländern betroffen waren und auch den Betrieb einiger britischer Krankenhäuser tangierte (Darf Google mit Patientendaten forschen? www.faz.net 17.05.2017).

USA

Digitalassistenten bekommen zunehmend gerichtliches Gehör

Daten der Computer-Sprachassistentin „Alexa" des Internethändlers Amazon wurden in den USA erstmals in einer Mordermittlung ausgewertet. Der US-Konzern gab seinen Widerstand gegen den entsprechenden Antrag der Ermittlungsbehörden bei einem Gericht im US-Bundesstaat Arkansas auf, nachdem der Tatverdächtige selbst der Herausgabe der Informationen zugestimmt hatte. In dem Fall war ein Bekannter des Mannes im Herbst 2015 nach einer durchzechten Nacht tot in dessen Whirlpool gefunden worden. Die Ermittler vermuteten einen vertuschten Mord, der Angeklagte wies die Anschuldigungen zurück. Die Polizei erhoffte sich von den Daten aus Amazons Netz-Kommunikationssystem „Echo" unter anderem Informationen darüber, ob jemand in der Nacht im Haus wach war und die Assistentin Alexa aktiviert haben könnte. Der Beschuldigte hatte erklärt, dass er geschlafen und seinen Bekannten erst am Morgen tot vorgefunden habe. Das Echo-System hat sieben Mikrofone, die darauf warten, dass das Schlüsselwort „Alexa" fällt. Daraufhin aktiviert sich das Gerät und schickt die Sprachbefehle zur Verarbeitung in die Cloud weiter. Auf Wunsch des Besitzers bestellt Alexa dann neues Waschmittel, dimmt das Licht in der Küche oder dreht die Heizung im durchdigitalisierten Haushalt herab. Auch wenn Alexa gerade nichts zu tun hat, hört der Assistent zu und kann so Zeuge eines Mordes werden.

Digitale Assistenten sind auch smarte Fernseher, Fitnessarmbänder oder Herzschrittmacher, die Daten mit gerichtlicher Beweiskraft speichern. So hatte ein Mann behauptet, er sei beim Brand seines Hauses durch ein Fenster geflüchtet. Die aufgezeichneten Messungen seines Herzschrittmachers konnten die Behauptung nicht belegen. Der Herzpatient wurde stattdessen der Brandstiftung verdächtigt. In Pennsylvania widersprachen die Daten des Fitnessarmbandes einer Frau ihrer Behauptung, angegriffen worden zu sein. Die Behörden ließen den Fall deshalb fallen.

DatenschützerInnen warnen vor den allgegenwärtigen Spionen. Digitalforensiker John Sammons von der Marshall University demonstrierte auf einem Kongress in New Orleans, was man aus dem Speicher eines modernen Autos auslesen kann: das Adressbuch des angeschlossenen Mobiltelefons, Anrufliste und Textnachrichten, außerdem die Position des Autos, wann gebremst und wann die Türen geöffnet wurden. Sammons bezeichnet die heutigen Möglichkeiten als „Spitze des Eisbergs". Mit dem Trend, Alltagsgegenstände ans Internet anzuschließen, gerate die Privatsphäre zunehmend in Gefahr (Sprachdienst als Zeuge, SZ 08.03.2017, 8; Charisius, Zeuge am Handgelenk, SZ 21.03.2017, 14).

USA

Arbeitgeber dürfen Gentest fordern

Das US-Repräsentantenhaus hat einem Gesetzentwurf zugestimmt, der es Unternehmen erlaubt, künftig Bedienstete dazu zu nötigen, Gentests zuzustimmen und deren Ergebnisse offenzulegen. Amerikanische wie europäische Humangenetiker sind entsetzt und fordern, dass Gentests freiwillig erfolgen müssen. Die Europäische Gesellschaft für Humangenetik (ESHG) warnt vor einem Dammbruch mit dem Hinweis, dass Informationen über mögliche Erkrankungen der Privatsphäre zuzuweisen sind. Hintergrund des Protestes der ESHG ist die Befürchtung, dass Vorstöße im Bereich der Bioethik aus den USA nach Europa schwappen.

US-Unternehmen könnten nach dem neuen Gesetz firmeninterne Wellness-Programme als Schleichweg nutzen, um den gesetzlich festgelegten Schutz der genetischen Privatsphäre zu umgehen. Wer sich nicht an Programmen inklusive Gentest der Firmen beteiligt, wird mit deutlich höheren Krankenversicherungskosten überzogen. Wird über den Gentest ein erhöhtes Risiko für eine Erkrankung festgestellt und wären die Betroffenen so für die Unternehmen eine Belastung, so könnten diese die Arbeitsverträge nicht verlängern. In Deutschland wurde vor Jahren eine gesunde Lehrerin nicht verbeamtet, weil ihr Vater an der Erbkrankheit Chorea Huntington litt.

Humangenetiker fordern, dass genetische Profile nicht zur Grundlage für Bewertungen durch Arbeitgeber genommen werden dürfen. Zumeist lassen sich mit den Ergebnissen von Gentests nur Risiken feststellen ohne Gewissheit, dass eine Erkrankung erfolgen wird. Viele Menschen wollen nicht wissen, welche genetischen Belastungen sie mit sich herumtragen. Bei Ergebnissen zu einer sicheren Erkrankungen können die Betroffenen zumeist nichts tun, um der Erkrankung vorzubeugen oder diese hinauszuzögern (Viciano, Gentests sind Privatsache, SZ 18./19.03.2017, 33).

USA

Google muss Auslandsdaten offenlegen

Ein Amtsrichter in Philadelphia hat Google aufgetragen, E-Mails auf ausländischen Servern an das FBI zu übergeben. In einem ähnlichen Fall war das Software-Unternehmen Microsoft vor einem New Yorker Berufungsgericht erfolgreich, als es die Herausgabe der Daten von Servern in der Europäischen Union verweigerte und auf den Rechtsweg in der Europäischen Union (EU) verwies.

Der Richter argumentierte im Google-Fall, da Google ohnehin ständig Daten zwischen seinen Rechenzentren hin- und herkopiere, sei es ja nur nötig, die vom FBI angefragten Daten in die USA zu transferieren, sodass das FBI darauf zugreifen könne. Nichts spreche gegen eine Google-interne Übermittlung von E-Mails in die USA, die das Unternehmen in seinen internationalen Datenzentren speichere. Ein solcher Transfer beeinträchtige nicht die Rechte des Nutzers und stelle keinen Zugriff auf ausländische Daten dar. Zwar gebe es möglicherweise eine Verletzung der Privatsphäre, die geschehe aber beim Öffnen der Mails in den USA und nicht im Ausland. Google hatte erklärt, dass der Konzern aus technischen Gründen seine Daten auf verschiedene Server verteile. Deshalb sei mitunter gar nicht klar, wo einzelne E-Mails gespeichert seien.

Google teilte in einer Stellungnahme mit, dass der Richter von der bisherigen Rechtsprechung abgewichen sei und dass man gegen das Urteil Berufung einlegen werde. Man werde weiterhin gegen zu weitgehende Herausgabebeschlüsse vorgehen. Dem Urteil lässt sich entnehmen, dass Google jährlich rund 25.000 Auskunftsersuchen von Ermittlungsbehörden in den USA erhält (Mansmann, Google muss ausländische E-Mails an FBI übergeben, www.heise.de 05.02.2017; Google muss FBI mitlesen lassen, SZ 06.02.2017, 19).

USA

Opencnam sammelt weltweit Daten zum Verkauf übers Netz

Opencnam von der US-Firma Telo USA Inc. verkauft weltweit Daten an Dritte weiter, z. B. für einen halben Cent unsere Namen. Gemäß LinkedIn hat die 2015 gegründete Firma ihren Sitz in Atlanta und lediglich max. 50 Mitarbeitende. Das Unternehmen wirbt damit, dass es in den USA eine Telefonnummernabdeckung von 87% (204 Mio.) habe, weltweit außerhalb der USA immerhin noch von 57% (4,5 Mrd.) und in 229 Staaten seine Dienste bereitstelle. Auf der Seite www.opencnam.com kann jeder den Test machen und seine Telefonnummer eingeben. Bei vielen steht der volle Name, oder auch der Arbeitgeber. Über die Seite kann jeder selbst nachprüfen, was rauskommt, muss hierfür aber ein Konto einrichten. Die Frage ist, woher Opencnam diese Informationen, die an die Telefonnummer gekoppelt sind, bezieht. Opencnam antwortete auf Nachfrage, sie kämen aus „non-traditionel sources“. Der Vorsitzender der Deutschen Vereinigung für Datenschutz, Frank Spaeing, vermutet, dass die Daten von Apps stammen, die sich vorher von dem Nutzenden wissentlich oder unwissentlich Zugang zum Telefonbuch haben gewähren lassen. Wenn da also ein Name steht und so etwas wie „Hanna, Freundin von Klaus“, dann kann daraus geschlossen werden, dass jemand Hanna so in seinem Adressbuch auf dem Smartphone abgespeichert hat, sich irgendwann mal eine (vermutlich) kostenlose App runtergeladen hat und diese App die Daten dann weiterverkauft hat, zum Beispiel an Opencnam, das sie wiederum weiter verkauft.

Dass auf die Daten aus dem Smartphone zugegriffen wird, steht meist in den AGB, genauso wie, dass diese Daten an Dritte weiter gegeben werden dürfen. Die meisten stimmen unwissend zu, weil sie die AGB nicht gelesen haben. Man kann natürlich zur zuständigen Datenschutzbehörde gehen, viel macht die aber selten, wenn wie hier das Unternehmen seinen Sitz in den USA hat. Dessen ungeachtet wäre es möglich, über die Europäische Kommission insofern Druck auszuüben (Opencnam weiß, wie du heißt, dradiowissen.de 01.02.2017).

USA

Klage gegen Bose wegen Kopfhörerspionage

Der Edelradiohersteller Bose soll einer Klage zufolge mit Apps für seine Funkkopfhörer die Privatsphäre seiner KundInnen verletzt haben. In der Klageschrift, die am 18.04.2017 bei einem Bundesgericht in Chicago eingereicht wurde, heißt es, das Unternehmen aus dem US-Bundesstaat Massachusetts missachte den Datenschutz bei seiner Software. Geplant ist demnach eine Sammelklage. In der Klage geht es um eine kostenlose Software namens Bose Connect, die sich die KundInnen kostenlos auf ihr iPhone oder Android-Smartphone laden können. Darüber sammele das Unternehmen Daten über Musik, Podcasts und andere Dateien, die sich die KundInnen anhörten, und leite diese Informationen an andere Firmen weiter. Der Kläger Kyle Zak hatte sich nach eigenen Angaben einen Bose-Kopfhörer für 350 Dollar gekauft. Er beantragte, dass Bose Käufern der entsprechenden Geräte Schadenersatz in Millionenhöhe leistet (Spionage über Kopfhörer, SZ 21.04.2017, 19)



USA/Kanada

Sammelklage gegen Vibratoren-App bringt 5 Millionen kanadische Dollar

Die kanadische Firma „Standard Innovation" hat gegen Zahlung von 5 Millionen kanadische Dollar einen Rechtsstreit in den USA um die Sammlung höchst intimer Daten durch seine Reihe smarter Vibratoren namens We-Vibe beigelegt (vgl. DANA 4/2016, 198). Die zum Steuern der Sexspielzeuge nötige We-Connect-App schickte der Sammelklage zufolge heimlich Nutzungsdaten an den Hersteller – darunter auch, wie oft und wann das Gerät verwendet wurde, die Intensität der Vibration sowie die eingestellte Temperatur.

Teilweise laufen die über Bluetooth mit dem Smartphone verbundenen Produkte ausschließlich mit dieser Anwendung; diese sorgt zudem für einen erheblichen Teil des Funktionsumfangs. Das Programm erlaubt unter anderem die Steuerung der Vibrationsmuster und -stärke. Die App eignet sich auch zu Steuerung des verbundenen Geräts aus der Ferne über das Internet. Nutzende können sich über Video- und Textchat mit der PartnerIn austauschen. Alles läuft über die Server der Herstellerfirma. Viele Funktionen verlangten eine Registrierung mit einer Mail-Adresse. Der Hersteller bestritt das Sammeln von Daten nicht, betonte jedoch zur Klageeröffnung, dass die Daten grundsätzlich nicht personenbezogen seien und sicher vor fremden Zugriffen gespeichert würden. Es habe bisher keine erfolgreichen Angriffe auf die Daten gegeben.

Die beiden Kläger, die zum Schutz der Privatsphäre als NP und PS vor Gericht erschienen, vertraten dagegen die Meinung, dass die gesammelten Daten sehr wohl zugeordnet werden können. Das Sammeln verstoße untere anderem gegen mehrere Gesetze im US-Bundesstaat Illinois und gegen ein Überwachungsgesetz auf Bundesebene. Zudem hätten die Käufer vor dem Kauf nicht wissen können, dass für die Verwendung des Geräts das Sammeln und Überwachen dieser Daten notwendig sei. Standard Innovation rechtfertigte zu Beginn des Verfahrens die Datensammlung unter anderem mit seiner Marktforschung: Wenn die Nutzer das Gerät überwiegend auf der höchsten Stufe nutzen würden, könnte das Gerät allgemein zu schwach zu sein.

Betroffene Kunden in den USA müssen gemäß der Vereinbarung zur Klagebeilegung zwischen zwei Arten der Entschädigung wählen: Wer die App zum Steuern der Geräte benutzt hat und Name, Mail-Adresse und Telefonnummer angibt, hat Anspruch auf bis zu 10.000 US-Dollar. Die genaue Höhe berechnet sich nach der Zahl der betroffenen Kunden. Knapp 3 Millionen US-Dollar (oder 4 Millionen kanadische Dollar) hat die Firma dazu beiseite zu legen. Wer das Gerät nur gekauft hat, erhält bis zu 199 US-Dollar zurück, wofür 1 Million kanadische Dollar zur Verfügung stehen.

Standard Innovation zeigte sich über die Beilegung der Sammelklage erleichtert und verwies auf seine verbesserte App: So kläre man deutlicher über die Datensammlung auf, die Sicherheit der App sei erhöht wurden und der Nutzer habe mehr Möglichkeit zum Steuern der Datenübertragung. Seit Oktober müssen Nutzer kein Konto mehr anlegen und können das Teilen der Daten abstellen. Zudem „arbeitete man mit führenden Experten für Sicherheit und Datenschutz weiter an der Verbesserung der App" (Spier, Smarte Vibratoren zu neugierig: We-Vibe zahlt Millionen-Entschädigung, www.heise.de 11.03.2017).

China

Gesichtsscanner kontrollieren Klopapiernutzung auf Toiletten

In Rahmen von Chinas Bürgerzivilisierungskampagne wird inzwischen versucht, den Diebstahl von kostenlosem Toilettenpapier mit Gesichtsscanner zu bekämpfen. Seit 2007, ein Jahr vor den Olympischen Spielen in Peking, war auf einigen Toiletten in China die uralte Regel außer Kraft gesetzt worden, wonach jeder Pekinger und jeder Tourist stets sein eigenes Papier am Leibe zu tragen hatte. In manchen Toiletten wurden Papier-Rollen in Griffweite bereitgestellt als „Willkommen an die Olympiagäste". Dies verstanden einige Chinesen als Einladung zum Abstauben, wie eine Schlagzeile der Pekinger „Global Times" im Jahr 2012 zeigte: „Kein Ende in Sicht beim Problem der Toilettenpapierdiebe". Jetzt teilte die Volkszeitung mit: „Noch immer mangelt es einigen Leuten an Papierbenutzungsmanieren." Sie klauen das Papier und nehmen es mit nach Hause. Deshalb ist von den 12.000 öffentlichen Toiletten der Stadt nur jede vierte mit Papier bestückt. Einige der Toiletten im Pekinger Himmelspark waren im Zuge der seit vielen Jahren laufenden „Toilettenrevolution" (so die offizielle Bezeichnung durch die Stadtregierung) zu „Vier-Sterne-Toiletten" ausgebaut worden.

Anfang März 2017 hatten sich in einer von ihnen Reporter der Pekinger Abendzeitung mit versteckter Kamera auf die Lauer gelegt. Sie beobachteten Leute, die in aller Seelenruhe bis zu zehn Meter Klopapier abrollten. Manche standen dafür Schlange und hatten Taschen mitgebracht, in die sie die Beute einpackten. Eine Frau kam innerhalb einer halben Stunde gleich drei Mal. Wenn man der Lokalpresse glauben darf, waren es alles Pensionäre aus der Umgebung, eine Rentnergang, die öffentliches Eigentum „kollektivierte", so einige Zeitungen.

Es folgte ein öffentliches Moralisieren über die „nationale Tragödie" (so ein Nutzer im Kurznachrichtendienst Weibo), also den fehlenden Gemeinsinn. Eine neue Kampagne der Stadtverwaltung erklärte die Park-Toilette zum „sichtbaren Zeugnis des Standes der Aufbau der geistigen Zivilisation" und schlug als Parole für den bevorstehenden Kampf das Motto vor: „Zivilisierte Toilettennutzung fängt bei mir an, fängt sofort an, fängt bei einem Blatt Papier an".

Der Parteisekretär der Himmelstempelparkverwaltung, Dong Yali, gab eine Pressekonferenz, in der er die Fluchtiraden und sogar Prügel beschrieb, mit der jene Mitarbeiter zu rechnen hätten, die versuchten, sich den Abrollern in den Weg zu stellen. Er kündigte an, man werde die Angestellten in Deeskalation schulen, zudem sollten neue Schilder und Freiwillige den Besuchern nahebringen, „wie man zivilisiert Toilettenpapier benützt".

Herr Dong verriet damals nicht, dass zudem der Große Bruder übers korrekte Geschäft wachen sollte. Die auto-

matischen Toilettenpapierspender im Vorraum von insgesamt sechs Mustertoiletten sind seit dem 18.03.2017 für zwei Wochen auf Probe mit Gesichts-Scannern gekoppelt. Wer Klopapier ziehen will, der muss vor eine Kamera treten und sein Gesicht einlesen lassen, dann erhält er genau 60 Zentimeter zugeteilt und ist für die nächsten neun Minuten gesperrt. In der Praxis versagten einige der Apparate gleich am ersten Tag. Andere brauchten nicht „ein paar Sekunden“ wie versprochen für die Gesichtserkennung, sondern mehr als eine Minute, was, wie eine Zeitung feststellte, „manchen, den es drängt, zusätzlich frustrieren kann“. Die Angestellten, die als Helfer neben den neuen Apparaten postiert waren, hatten viel zu tun. Ob die Aktion am Ende erfolgreich ist, bezweifelten viele Internetnutzer in einer angeregten öffentlichen Diskussion in sozialen Medien. Das langfristige Schicksal der Gesichtsscanner ist noch unklar. Ein Vertreter der Parkverwaltung versprach aber der Presse, dass das kostenlose Klopapier nicht abgeschafft wird: „Das ist eine Sache der Menschlichkeit“ (Strittmatter, SZ 21.03.2017, 8).

China

Jack Ma investiert in Gentests

Der Gründer des Onlinehändlers Alibaba und zugleich reichster Chinese Jack Ma investiert viele Millionen in die Genanalysefirma Wuxi Nextcode und damit im boomenden Markt der Erbgutentschlüsselung. Das Unternehmen ist aus dem deCode-Projekt in Island entstanden, in dem die Erbinformationen von 140.000 Freiwilligen erfasst und auf Krankheitsmarker hin untersucht worden waren. Die Pharmaforschung hofft, mithilfe solcher Datensätze innovative Medikamente entwickeln zu können. Zudem entwickelt sich ein Markt für Gentests, die sich direkt an KonsumentInnen richten. Wuxi Nextcode werden große Chancen auf dem Endverbrauchermarkt zugeschrieben, u. a. weil es in China in diesem Bereich keine bzw. nur eine lasche rechtliche Regulierung gibt (Alibaba-Gründer setzt auf Gentests, Der Spiegel 19/20017, 57)

Rechtsprechung

EuGH

Bei Gesellschaftsregistern nur eingeschränktes Recht auf Vergessenwerden.

Mit Beschluss vom 09.03.2017 urteilte der Europäische Gerichtshof (EuGH), dass es kein „Recht auf Vergessenwerden“ für die im Gesellschaftsregister eingetragene personenbezogenen Daten gibt (C-398/15). Die Mitgliedstaaten können aber nach Ablauf einer hinreichend langen Frist nach der Auflösung der betreffenden Gesellschaft in Ausnahmefällen eine Beschränkung des Zugangs Dritter zu diesen Daten vorsehen. Geklagt hatte 2007 der Geschäftsführer einer Gesellschaft gegen die Handelskammer Lecce, die einen öffentlichen Auftrag für die Errichtung einer Ferienanlage in Italien erhalten hatte. Er war der Auffassung, dass sich die Immobilien der Anlage deshalb nicht veräußern ließen, weil sich aus dem Gesellschaftsregister ergebe, dass er Geschäftsführer einer anderen Gesellschaft gewesen sei, die 1992 insolvent geworden und 2005 liquidiert worden sei.

Das erstinstanzliches Gericht in Italien gab der Handelskammer Lecce auf, die personenbezogenen Daten zu anonymisieren, die den Kläger mit der Insolvenz der früheren Gesellschaft in Verbindung bringen, und verurteilte die Handelskammer zum Ersatz des dem Kläger daraus entstandenen Schadens. Der von der Handelskammer Lecce angerufene Kassationsgerichtshof hat dem EuGH mehrere Fragen zur Vorabentscheidung vorgelegt. Er wollte wissen, ob es die Richtlinie 95/46/EG zum Schutz der Daten natürlicher Personen und die Richtlinie 68/151/EWG über die Offenlegung von Gesellschaftsurkunden verbieten, dass jede Person ohne zeitliche Beschränkung Zugang zu natürliche Personen betreffenden Daten im Gesellschaftsregister haben kann.

Der EuGH wies darauf hin, dass die Offenlegung von Gesellschaftsregistern die Rechtssicherheit in den Beziehungen zwischen den Gesellschaften und Dritten sicherstellen soll und u.a. dazu dient, die Interessen Dritter gegenüber Aktiengesellschaften und Gesellschaften mit beschränkter Haftung zu schützen, da diese zum Schutz Dritter lediglich ihr Gesellschaftsvermögen zur Verfügung stellen. Außerdem können sich auch noch mehrere Jahre nach Auflösung einer Gesellschaft Fragen ergeben, die einen Rückgriff auf im Gesellschaftsregister eingetragene personenbezogene Daten erfordern. In Anbetracht der Vielzahl der Rechte und Rechtsbeziehungen, die eine Gesellschaft (auch nach ihrer Auflösung) mit Akteuren in mehreren Mitgliedstaaten verbinden können, und der Unterschiede in den Verjährungsfristen der verschiedenen nationalen Rechte sei es nicht möglich, eine einheitliche Frist festzulegen, nach deren Ablauf die Eintragung der Daten im Register und ihre Offenlegung nicht mehr notwendig wären.

Unter diesen Umständen können die Mitgliedstaaten natürlichen Personen, deren Daten im Gesellschaftsregister eingetragen sind, nicht das Recht garantieren, nach einer bestimmten Frist nach Auflösung der Gesellschaft die Löschung der sie betreffenden personenbezogenen Daten verlangen zu können. Dieser Eingriff in die Grundrechte der betroffenen Personen (Achtung des Privatlebens und Schutz personenbezogener Daten) sei nicht unverhältnismäßig, da erstens nur eine begrenzte Zahl an personenbezogenen Daten im Gesellschaftsregister eingetragen wird und es zweitens gerechtfertigt ist, dass die natürlichen Personen, die sich dafür entscheiden, über eine Aktiengesellschaft oder eine Gesellschaft mit beschränkter Haftung am Wirtschaftsleben teilzunehmen, und die zum Schutz Dritter lediglich das Vermögen dieser Gesellschaft zur Verfügung stellen, verpflichtet sind, die Daten zu ihren Personalien und Aufgaben innerhalb der Gesellschaft offenzulegen.

Allerdings sei es nicht auszuschließen, dass in besonderen Situationen überwiegende, schutzwürdige, sich aus

dem konkreten Fall der Person ergebende Gründe ausnahmsweise rechtfertigen können, den Zugang zu den sie betreffenden personenbezogenen Daten nach Ablauf einer hinreichend langen Frist nach der Auflösung der Gesellschaft auf Dritte zu beschränken, die ein besonderes Interesse an der Einsichtnahme in die Daten nachweisen. Eine solche Zugangsbeschränkung zu personenbezogenen Daten müsse das Ergebnis einer Einzelfallprüfung sein. Es sei Sache jedes Mitgliedstaats, zu entscheiden, ob er eine solche Zugangsbeschränkung in seiner Rechtsordnung wünscht. Vorliegend kann der Umstand allein, dass sich die Immobilien der Ferienanlage nicht veräußern lassen, weil die potenziellen KäuferInnen Zugang zu den im Gesellschaftsregister eingetragenen Daten über den Kläger haben, u. a. wegen des berechtigten Interesses dieser Käufer an diesen Informationen nicht für eine Rechtfertigung der Zugangsbeschränkung zu diesen Daten ausreichen (Kein Recht auf Vergessenwerden hinsichtlich der im Gesellschaftsregister eingetragenen personenbezogenen Daten, www.otto-schmidt.de 09.03.2017).

BVerfG

Pressefotos Prominenter nur im öffentlichen Raum zulässig

Manchmal liegen zwischen Recht und Unrecht nur ein paar Meter. Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 09.02.2017 über zwei in der Bild-Zeitung abgedruckte Aufnahmen aus dem Jahr 2011 entschieden und damit die Grenze zwischen Pressefreiheit und Persönlichkeitsschutz sehr anschaulich gemacht (1 BvR 2897/14, 1 BvR 790/15, 1 BvR 967/15). Während seines Vergewaltigungsprozesses, der 2011 mit Freispruch endete, war der Wettermoderator Jörg Kachelmann von Fotografen verfolgt worden; gegen viele veröffentlichte Fotos ist er vor Gericht gezogen. Eine der Aufnahmen, veröffentlicht am 18.05.2011, zeigt Kachelmann auf dem Weg zu seiner Verteidigerin, auf öffentlicher Straße, wenige Meter vor der Kanzlei. Land- und Oberlandesgericht Köln sahen darin einen erheblichen Eingriff in seine Privatsphäre. Das BVerfG hob die Entscheidung wegen Verletzung der Pressefreiheit auf. Dass das Foto geringen Informationswert habe, sei nicht entscheidend. Zudem gehöre es zur Freiheit der Presse, „nach publizistischen Kriterien zu entscheiden, was öffentliches Interesse beansprucht“. Das Gericht hob hervor, dass ein Prominenter, der in einen Fall von allergrößtem öffentlichen Interesse verwickelt war, nun mal keine Privatsphäre genießt, solange er sich im öffentlichen Raum bewegt. Auf dem Parkplatz im ein wenig abgeschirmten Innenhof der Kanzlei war Kachelmann auch abgelichtet worden. Dort befinde er sich in einer „durch räumliche Privatheit geprägten Situation“, befand das Gericht und wies die Verfassungsbeschwerde von „Bild“ ab (Janisch, SZ 16.03.2017, 47).

BVerfG

Weitere Eilanträge gegen Vorratsdatenspeicherung abgelehnt

Das Bundesverfassungsgericht (BVerfG) hat erneut Eilanträge auf Erlass einer einstweiligen Anordnung gegen das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.12.2015 mit Beschlüssen vom 26.03.2017 abgelehnt (1 BvR 3156/15, 1 BvR 141/16). Die Antragsteller wollten insbesondere mit Blick auf das Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 21.12.2016 (C-203/15, C-698/15, DANA 1/2017, 60) erreichen, dass die durch dieses Gesetz eingeführte Vorratsspeicherung von Telekommunikations-Verkehrsdaten zu Zwecken der öffentlichen Sicherheit außer Kraft gesetzt wird. Nach Ansicht des BVerfG stellen sich auch nach der Entscheidung des EuGH hinsichtlich der verfassungsrechtlichen Bewertung der angegriffenen Regelungen Fragen, die nicht zur Klärung im Eilrechtschutzverfahren geeignet seien.

Aufgrund einer Übergangsfrist beginnt die Speicherpflicht am 01.07.2017. Dann müssen Internet-Firmen 10 Wochen lang speichern, wer sich wann mit welcher IP-Adresse im Internet eingeloggt hatte. Telefonfirmen müssen 10 Wochen lang festhalten, wer wann mit wem telefoniert oder gesimst hat. Die Standortdaten bei der Mobilkommunikation müssen 4 Wochen lang gespeichert werden. Am 08.06.2016 hatte das BVerfG erstmals Eilanträge gegen die Wiedereinführung der Vorratsdatenspeicherung abgelehnt (DANA 3/2016, 153 f.). Zwar könne die anlasslose Datenspeicherung einen „erheblichen Einschüchterungseffekt“ bewirken, weil das Gefühl entstehe, „ständig überwacht zu werden“. In einer Folgenabschätzung sprach sich das Gericht aber gegen den vorläufigen Stopp des Gesetzes aus.

Neuer Schwung kam in die Debatte durch die Feststellung des EuGH im Dezember 2016, dass die Vorratsspeicherung in Großbritannien und Schweden nicht mit EU-Recht vereinbar ist. Der EuGH verlangte einen zumindest mittelbaren Zusammenhang der gespeicherten Personen mit schweren Straftaten oder deren Verhütung. Die Gegner der Vorratsdatenspeicherung schöpften Hoffnung und reichten zwei Eilanträge ein. Der eine stammte von 22 Berliner Anwälten, Journalisten und Abgeordneten; der andere wurde vom SPD-nahen Verein für digitalen Fortschritt D64 eingereicht. Beide Anträge wurden nun von einer Kammer des BVerfG abgewiesen. Anhängig bleibt ein Versucht des Münchener Providers SpaceNet AG, der verhindern will, dass er für 40.000 € neue Speicher-Hardware anschaffen muss. Der deshalb gestellte Eilantrag wurde Ende Januar 2017 vom Verwaltungsgericht Köln abgelehnt, wogegen SpaceNet beim Oberverwaltungsgericht Münster Rechtsmittel eingelegt hat (Rath, Vorratsdatenspeicherung kann starten, Kieler Nachrichten 15.04.2017, 4; BVerfG, PE Nr. 28/2017 v. 25.03.2017, Weitere Eilanträge in Sachen „Vorratsdatenspeicherung“ erfolglos).

BGH

IP-Adressenspeicherung für Sicherheitszwecke zulässig

Der Bundesgerichtshof (BGH) in Karlsruhe entschied mit Urteil vom 16.05.2017, dass bedrohte Webseiten

Surfprotokolle ihrer Nutzenden zur Abwehr von Sicherheitsrisiken anlegen dürfen (Az. VI ZR 135/13). Der Kläger, der bisherige Abgeordnete der Piraten im Schleswig-Holsteinischen Landtag Patrick Breyer (die Piraten schafften es bei der Wahl am 07.05.2015 nicht wieder in den Landtag), verlangte vor ca. 10 Jahren von der beklagten Bundesrepublik Deutschland die Unterlassung der Speicherung von dynamischen IP-Adressen. Diese Ziffernfolgen werden bei jeder Einwahl ins Internet dem jeweiligen Rechner zugewiesen, um diesem die Kommunikation zu ermöglichen. Bei einer Vielzahl allgemein zugänglicher Internetportale des Bundes werden alle Zugriffe in Protokolldateien festgehalten mit dem Ziel, Angriffe abzuwehren und die strafrechtliche Verfolgung von Angreifern zu ermöglichen. Dabei werden unter anderem der Name der abgerufenen Seite, der Zeitpunkt des Abrufs und die IP-Adresse des zugreifenden Rechners über das Ende des jeweiligen Nutzungsvorgangs hinaus gespeichert.

Breyer forderte vom Bund es zu unterlassen, ihm zugewiesene IP-Adressen über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern. Das Amtsgericht hatte die Klage abgewiesen; auf die Berufung des Klägers hin hatte dann das Landgericht (LG) dem Kläger den Unterlassungsanspruch insoweit zuerkannt, als er Speicherungen von IP-Adressen in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs betrifft und der Nutzer während des Nutzungsvorgangs seine Personalien angibt. Gegen dieses Urteil hatten beide Parteien die vom LG zugelassene Revision eingelegt.

Der BGH setzte darauf mit Beschluss vom 28.10.2014 das Verfahren aus und legte dem Europäischen Gerichtshof (EuGH) zwei Fragen zur Auslegung der EG-Datenschutz-Richtlinie (Richtlinie 95/46 EG – EG-DSRl) zur Vorabentscheidung vor. Nachdem der EuGH die Fragen mit Urteil vom 19.10.2016 (C-582/14) beantwortet hatte, hob der BGH nunmehr im Rahmen der Revisionen das Berufungsurteil auf und verwies die Sache an das Berufungsgericht zurück.

Auf der Grundlage des EuGH-Urteils bestätigte der BGH, dass das Tatbestandsmerkmal „personenbezogenes Datum“ des § 12 Abs. 1 und 2 TMG in Verbindung mit § 3 Abs. 1 BDSG richtlinienkonform so auszulegen ist, dass darunter auch eine dynamische IP-Adresse fällt, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Internetseite, die dieser Anbieter allgemein zugänglich macht, gespeichert wird. Als solches darf die IP-Adresse nur unter den Voraussetzungen des § 15 Abs. 1 TMG gespeichert werden. Diese Vorschrift ist, so folgt der BGH dem EuGH, entsprechend Art. 7 lit. f EG-DSRl dahingehend auszulegen, dass ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus verarbeiten darf, soweit dies erforderlich ist, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten. Dabei sei allerdings einer Abwägung mit dem Interesse und den Grundrechten und -freiheiten der Nutzenden vorzunehmen.

Diese Abwägung konnte vom BGH im Streitfall auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen nicht abschließend vorgenommen werden. Das Berufungsgericht hatte keine hinreichenden Feststellungen dazu getroffen, ob die Speicherung der IP-Adressen des Klägers über das Ende eines Nutzungsvorgangs hinaus erforderlich ist, um die (generelle) Funktionsfähigkeit der jeweils in Anspruch genommenen Dienste zu gewährleisten. Der beklagte Bund verzichtet nach eigenen Angaben bei einer Vielzahl der von ihm betriebenen Portale mangels eines „Angriffsdrucks“ darauf, die jeweiligen IP-Adressen der Nutzenden zu speichern. Es fehlte insbesondere an Feststellungen dazu, wie hoch das Gefahrenpotential bei den übrigen Online-Mediendiensten des Bundes ist, welche Breyer nutzen möchte. Erst wenn entsprechende Feststellungen hierzu getroffen sind, kann das LG als Berufungsgericht die nach dem Urteil des EuGH gebotene Abwägung zwischen dem Interesse der Beklagten an der Aufrechterhaltung der Funktionsfähigkeit ihrer Online-Mediendienste und dem Interesse oder den Grundrechten und -freiheiten des Klägers vornehmen haben. Dabei sind, so der BGH, Gesichtspunkte der Generalprävention und der Strafverfolgung gebührend zu berücksichtigen.

Das Urteil hat über die betroffenen Regierungsportale hinausgehende Bedeutung auch für viele Unternehmen, die Nutzungsdaten aus Sicherheitsgründen speichern. Breyer sieht weiterhin keinen Sicherheitsgewinn in einer Speicherung: „Ein effektiver Schutz vor Angriffen ist alleine durch technische Absicherung der Systeme möglich“. Deshalb sei es unverhältnismäßig, die Anonymität im Netz aufzuheben. Der Branchenverband Bitkom hält demgegenüber die Speicherung für nützlich, so das Mitglied der Geschäftsführung Susanne Dehmel: „Einen anderen Anhaltspunkt als die IP-Adresse hat man oft nicht.“ Die Daten ließen sich aber ohnehin nur für einen begrenzten Zeitraum beim Provider abrufen (Bundesgerichtshof zur Zulässigkeit der Speicherung von dynamischen IP-Adressen, BGH PE Nr. 74/2017 v. 16.05.2017; Janisch, Alles für die Sicherheit, SZ 17.05.2017, 17).

LAG Berlin-Brandenburg

Fristlose Kündigung wegen Datenschutzverstoß

Mit Urteil vom 01.09.2016 bestätigte das Landesarbeitsgericht (LAG) Berlin-Brandenburg einen vermehrt erkennbaren Trend der Rechtsprechung, Datenschutzverstöße nicht mehr als Kavaliersdelikte, sondern als schwere Pflichtverletzung anzusehen, die eine fristlose Kündigung rechtfertigt (10 Sa 192/16). Eine Mitarbeiterin eines Berliner Meldeamtes hatte mehrere hundert Melderegisterabfragen zu Personen aus ihrem näheren Bekanntenkreis vorgenommen und damit gegen datenschutzrechtliche Anforderungen verstoßen. Das Amtsgericht Berlin-Tiergarten verurteilte sie wegen der begangenen Datenschutzverletzung zu einer Geldstrafe von 90 Tagessätzen. Das Land Berlin als Arbeitgeber kündigte ihr fristlos. Diese Kündigung wurde zwar vom Arbeitsgericht (ArbG) Berlin (56 Ca 6036/15) aufgehoben mit dem Verweis, die Klägerin habe ohne kriminelle Energie gehandelt. Diese hatte vorgetragen, ihr sei der Datenschutzverstoß nicht bewusst gewesen; sie habe aus reiner Neugier gehandelt.

Das LAG hob die Entscheidung des ArbG auf und bestätigte die Kündigung.

Die Mitarbeiterin habe ihre vertraglichen Pflichten verletzt. Für eine solche Kündigung aus einem wichtigen Grund gemäß § 626 Abs. 1 Bürgerliches Gesetzbuch (BGB) kommt es auf einen Verstoß gegen die vertraglichen Haupt- oder Nebenpflichten und den damit verbundenen Vertrauensbruch an. Der von der Klägerin begangene Verstoß gegen datenschutz- und melderechtliche Vorschriften rechtfertige die fristlose Kündigung. Daran könne auch die langjährige beanstandungslose Beschäftigung beim Land nichts ändern. Den bei der Meldebehörde beschäftigten Personen ist es gesetzlich untersagt, die ihnen für die Erfüllung ihrer Aufgaben zur Verfügung gestellten Meldedaten unbefugt zu einem anderen Zweck als dem der rechtmäßigen Aufgabenerfüllung zu verarbeiten. Die Klägerin hatte die Persönlichkeitsrechte der Personen, deren Daten sie unbefugt abgerufen hat, und das Datengeheimnis, auf das sie verpflichtet war, verletzt (Wybitul, Sind Verstöße gegen den Datenschutz Kavaliersdelikte? www.faz.net 09.02.2017; Wurzberger CuA 3/2017, 23).

LG Köln

Rekordschadenersatz für Kohl wegen Persönlichkeitsverletzung

Das Landgericht (LG) Köln hat mit Urteilen vom 27.04.2017 dem früheren Bundeskanzler Helmut Kohl einen Rekord-Schadenersatz in Höhe von einer Million Euro zugesprochen und bestätigte das Verbot von 116 Textpassagen des Bestsellers „Vermächtnis: Die Kohl-Protokolle“ (14 O 323/15, 14 O 286/14, 14 O 261/16). Die Veröffentlichung des Buches hat nach Auffassung des Gerichts das Persönlichkeitsrecht des 87-Jährigen schwer verletzt. In den beanstandeten Textpassagen ging es um vertrauliche Äußerungen Kohls über andere bekannte Politiker und Persönlichkeiten des öffentlichen Lebens. Von den 116 im Prozess behandelten Zitaten waren 13 von Kohl bestritten worden.

In dem Zivilverfahren hatte Kohl die Autoren Heribert Schwan und Tilman Jens sowie den Heyne-Verlag aus der Verlagsgruppe Random House auf Zahlung von fünf Millionen Euro verklagt. Die Verurteilung erfolgte gesamtschuldnerisch auf ein Fünftel, was aber in Deutschland absoluter Rekord ist. Die bisher höchsten Summen, die nach deutschem Recht für Verletzungen des Persönlichkeitsrechts durch unzulässige Veröffentlichungen zugesprochen wurden, bewegten sich um die 400.000 Euro, so im Fall des Wettermoderators Jörg Kachelmann und der Prinzessin Madeleine von Schweden. Im Fall Kachelmann hatte das LG Köln 635.000 Euro zugesprochen, was vom Oberlandesgericht Köln auf 395.000 reduziert wurde.

Die beanstandeten Aussagen stammen aus Gesprächen, die Kohl 2001 und 2002 mit Schwan über ca. 600 Stunden geführt hatte, damit der Journalist als Ghostwriter die Memoiren des Altkanzlers verfassen konnte. Schwan nahm die Gespräche auf Kassette auf. Bevor der vierte und letzte Band erscheinen konnte, zerstritten sich die beiden. Schwan veröffentlichte daraufhin eigenmächtig ein Buch mit pikanten Äußerungen Kohls aus ihren Gesprächen. Sie betrafen unter anderem die heutige Bundeskanzlerin Angela Merkel und die früheren Bundespräsidenten Christian Wulff und Richard von Weizsäcker. Zitiert wurde z. B. „Schaumschläger“, „trottelhaft katholisches Subjekt“, „Verräter“, „aus den Dessous herausgezogen“ oder „Er ist natürlich einer der Dreckigsten“. Das Buch wurde 2014 ein Bestseller und brachte es auf 200.000 verkaufte Exemplare. Kohl klagte jedoch dagegen und erreichte, dass es in der vorliegenden Form nicht mehr ausgeliefert werden durfte. Kohl hatte vorgebracht, seine Äußerungen seien strikt vertraulich gewesen. Schwan dagegen hatte immer erklärt, wenn Kohl etwas wirklich Vertrauliches gesagt habe, habe er ihn jedes Mal aufgefordert, den Kassettenrekorder auszustellen. Nach Überzeugung des Gerichts durfte nur Kohl selbst entscheiden, welche seiner Aussagen veröffentlicht werden sollten und welche nicht. Schwan habe mit dem Buch seine Verschwiegenheitspflicht und seine Pflicht zur Geheimhaltung verletzt. Die Höhe des Schadenersatzes begründete das Gericht mit eines „besonderen Schwere“ des Eingriffs in das Persönlichkeitsrecht. Der vorsitzende Richter Martin Koepsel erklärte, Kohl habe ein Recht auf Genugtuung. Dies wiege schwerer als das öffentliche Interesse. Zwar solle die Presse mit der Entscheidung nicht eingeschüchtert werden, doch müsse hier „eine spürbare Konsequenz“ folgen.

Die Schadenersatz-Entscheidung ist das Herzstück einer Reihe von Klagen, die alle mit der unerlaubten Veröffentlichung der Kohl-Zitate in Zusammenhang stehen. In einem separaten Verfahren hatte Kohl bereits 2015 die Herausgabe der Tonbänder erstritten, auf denen seine Gespräche mit Schwan aufgezeichnet waren. Mit Teilurteil wurde jetzt Schwan verpflichtet, Auskunft über Art, Umfang und Verbleib etwaiger Kopien dieser Tonbänder zu geben (14 O 286/14). Auf Grundlage dieser Auskunft wird Kohl sodann nach Auffassung der Kammer auch Herausgabe der Kopien fordern können. In einem weiteren Verfahren hatte Kohl zunächst per einstweilige Verfügung die Schwärzung der Zitate durchgesetzt, die nun im Hauptsacheverfahren bestätigt wurde (Urt. v. 27.04.2017, Az. 14 O 261/16).

Die Urteile sind noch nicht rechtskräftig. Die Anwälte der Autoren Heribert Schwan und Tilman Jens sowie des Verlags hatten schon vorher angekündigt, Rechtsmittel gegen die Entscheidung einzulegen, falls Kohls Klage stattgegeben werden sollte. Klägeranwalt Roger Mann sprach bzgl. der zugestandenen Forderung von einer „obszönen Summe, die man nicht ansatzweise nachvollziehen kann“ (LG Köln, Rekordentschädigung – Klagen wegen Veröffentlichungen aus den sog. „Kohl-Tonbändern“ in weiten Teilen erfolgreich, PM 27.04.2017; Altkanzler Kohl erhält Millionenentschädigung von Ex-Biograf Schwan, www.zeit.de 27.04.2017; Rekord-Schmerzensgeld für Helmut Kohl, www.lro.de 27.04.2017; Esslinger, Dafür soll er zahlen, SZ 28.04.2017, 5).

LG Würzburg

Facebook muss strafbare Fake-News nicht eigenständig löschen

Das Landgericht (LG) Würzburg wies am 07.03.2017 per Beschluss den Antrag des durch ein Selfie mit Bundeskanzlerin Angela Merkel (CDU) bekannt gewor-

denen syrischen Flüchtlings Anas Modamani auf Erlass einer einstweiligen Verfügung zurück, Facebook zu verpflichten, aktiv nach verleumderischen Fake-News zu suchen. Modamani wollte per einstweilige Verfügung Facebook zur Löschung der Falschmeldungen über ihn zwingen. Er hatte im September 2015 ein Selfie mit Kanzlerin Merkel gemacht, was wiederum auf einem Foto festgehalten ist. Dieses Bild wurde später für bei Facebook verbreitete Fotomontagen genutzt, in denen er mit Anschlägen und Verbrechen in Verbindung gebracht wurde. In einer dieser Montagen wurde er z. B. fälschlicherweise als mutmaßlicher Täter nach einem Brandanschlag auf einen Obdachlosen in Berlin dargestellt.

Das Landgericht stellte nicht infrage, dass es sich bei den auf Facebook verbreiteten Meldungen um Verleumdungen handelte. Facebook sei aber „weder Täter noch Teilnehmer", habe selbst weder etwas „behauptet" noch „verbreitet" und mache sich die Inhalte auch nicht zu eigen. Der vorsitzende Richter Volkmar Seipel meinte zur Begründung: „Es bleiben somit fremde Inhalte der Nutzer des Portals". Das aber sei Voraussetzung für eine einstweilige Verfügung. Die Richter setzten sich mit der Frage auseinander, ob Facebook möglicherweise aktiv nach solchen verleumderischen Falschmeldungen suchen muss. Bei einer „schweren Persönlichkeitsverletzung" erscheine ein „erhöhter Suchaufwand" grundsätzlich gerechtfertigt. Der Bundesgerichtshof (BGH) habe eine solche Verpflichtung aber nur dann bejaht, „wenn diese technisch ohne zu großen Aufwand realisierbar und damit zumutbar ist". Das Gericht sah sich nicht in der Lage, darauf in einem Eilverfahren eine Antwort zu finden. Diese Frage werde gegebenenfalls in einem Hauptsacheverfahren durch Gutachten zu klären sein. Die Richter sahen es für den Syrer als zumutbar an, eine Entscheidung in einem solchen Verfahren abzuwarten. Die strittigen Inhalte hätten bereits „weltweite Verbreitung" gefunden. Die Persönlichkeitsverletzung habe sich bereits ereignet und werde bis zu einem Hauptsacheverfahren nicht mehr gravierender werden. Es sei daher nicht erkennbar, dass weiterer Schaden drohe.

Seipel deutete an, dass Modamani in einem Hauptsacheverfahren zumindest teilweise Erfolg haben könne. Es sei unstreitig, dass es sich bei den Bildern und Collagen um strafbare Falschbehauptungen handle. Er äußerte Zweifel an der Argumentation der Facebook-Anwälte, dass Anas Modamis oder andere Verleumdungsopfer verpflichtet seien, jede einzelne Fundstelle der Bilder zu melden, bevor Facebook diese entfernen können. Es sei grundsätzlich denkbar, dass im Fall einer schweren Persönlichkeitsverletzung ein Portalanbieter von sich aus tätig werden müsse. Modamanis Würzburger Anwalt Chan-jo Jun wollte erreichen, dass Facebook selbständig nach den verleumderischen Bildern sucht und diese automatisch löscht oder gar das Hochladen verhindert. Seipel hielt das im Einzelfall für zumutbar, wenn das Vorgehen „technisch ohne zu großen Aufwand realisierbar" und nicht geschäftsschädigend sei. Die Facebook-Anwälte hatten bei der mündlichen Verhandlung behauptet, dazu brauche man eine „Wundermaschine". Ob es „diese ominöse Wundermaschine" gebe, so Seipel, müsste in einem Hauptsacheverfahren geklärt werden. Das Gericht ignorierte also, dass es schon seit langem Software gibt, die z. B. Kinderpornografie aus dem Netz filtert. Die verbotenen Bilder liegen hierfür in einer zentralen Datenbank. Der Beschluss führte zur journalistischen Forderung nach „mehr digitaler Bildung unter deutschen Richtern".

Ob es zu einem Hauptsacheverfahren kommt, blieb zunächst unklar. Modamanis Anwalt Jun kündigte an, dass er den Syrer dabei wegen persönlicher Angriffe über Facebook nicht weiter vertreten könne. Er zeigte sich „enttäuscht" darüber, dass die Bilder seines Mandanten weiter online seien. Das Gericht habe sich aber in den Grenzen bewegt, die das Gesetz vorsehe: „Wir brauchen andere Gesetze." Das geltende Recht reiche für die Opfer von Verleumdungen nicht aus. Die Würzburger Entscheidung habe gezeigt, dass der Weg über Gerichte nicht leicht ist.

Facebook zeigte sich zufrieden mit der Entscheidung. Ein Sprecher meinte, es freue das Unternehmen, „dass das Gericht unsere Ansicht teilt, dass die eingeleiteten rechtlichen Schritte hier nicht der effektivste Weg zur Lösung der Situation waren". Das Unternehmen verstehe „sehr gut", dass es für Modamani eine „schwierige Situation" sei. Facebook habe „schnell den Zugang zu Inhalten blockiert", die von seinem Anwalt „korrekt" gemeldet worden seien (Erfolg für Facebook in Würzburger Fake-News-Prozess, www.wochenblatt.de 07.03.2017; Henzler, Facebook muss Verleumdungen nicht suchen und löschen, SZ 08.03.2017, 1; Brühl, Märchenstunde, SZ 08.03.2017, 4).

VG Berlin

Klage gegen Handywegnahme bei Schüler unzulässig

Mit Urteil vom 04.04.2017 scheiterten ein Berliner Schüler und dessen Eltern vor dem Verwaltungsgericht (VG) Berlin mit ihrer Klage gegen eine Schule, in der der Schüler sein Handy dem Lehrer aushändigen musste (VG 3 K 797.15). Der Entzug eines Mobiltelefons durch einen Lehrer über mehrere Tage hinweg ist keine Verletzung von Grundrechten eines Schülers. Der Schüler hatte an einem Freitag in der letzten Schulstunde seinem Lehrer sein Handy aushändigen müssen, weil er sich damit unter der Bank damit beschäftigt hatte, statt dem Unterricht zu folgen. Die Schulleitung weigerte sich zunächst, das Mobiltelefon wieder herauszugeben und behielt es über das Wochenende unter Verschluss. Am darauffolgenden Montag konnte die Mutter des Schülers das Telefon abholen.

Die Eltern und der Schüler wollten mit ihrer Klage festgestellt wissen, dass die Einziehung und Verwahrung des Handys rechtswidrig war. Zudem sei der Schüler in seiner Ehre verletzt und gedemütigt worden. Das sahen die Richter anders. Sie stellten klar, dass die vom Schüler beklagte plötzliche Unerreichbarkeit per Telefon keine unzumutbare Beeinträchtigung seiner Grundrechte darstelle. Auch in das elterliche Erziehungsrecht sei damit nicht eingegriffen worden. Das Vorgehen der Schule stelle zudem keine Diskriminierung dar. Da der Schüler mittlerweile die Schule verlassen hat, werde sich der Vorfall nicht wiederholen. Die damals von Lehrer und Schulleitung getroffene „Maßnahme" könne nach der Rückgabe des Telefons „nicht ohne Weiteres auf ihre Rechtmäßigkeit überprüft werden". Der klagende Schüler, der

mittlerweile 18 Jahre alt ist, besuchte im Mai 2015 die neunte Klasse einer Sekundarschule in Berlin. Gegen das Urteil ist Berufung beim Oberverwaltungsgericht Berlin-Brandenburg möglich (Lehrer darf Handy von Schüler tagelang einziehen, www.rbb-online.de 17.05.2017, Mayer, Funkloch 18.05.2017).

AG Hamburg

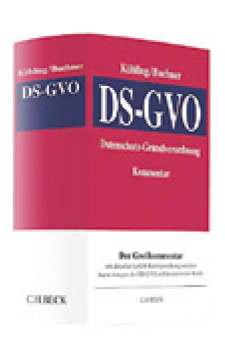
15.000 Euro Bußgeld wegen Geoscoring

Das Amtsgericht (AG) Hamburg bestätigte mit Beschluss vom 16.03.2017 einen Bußgeldbescheid des Hamburgischen Datenschutzbeauftragten (HmbBfDI) Johannes Caspar gegenüber dem Schufa-Konkurrenten Bürgel in Höhe von 15.000 € wegen Geoscoring (233 OWi 12/17). Die Hamburger Auskunftei Bürgel Wirtschaftsinformationen erhielt die Geldbuße, nachdem sie auf eine Bonitätsanfrage einer Online-Firma hin dieser allein einen Scorewert über die Wohnanschrift eines Kunden übermittelte. Weitere Auskünfte über die Person konnte sie nicht geben. Der HmbBfDI sah in dem Vorgehen einen klaren Verstoß gegen die gesetzlichen Vorgaben zum Scoring zur Prüfung der Kreditwürdigkeit.

Das Bundesdatenschutzgesetz (BDSG) untersagt es seit einer Reform von 2009 in § 28b, „ausschließlich“ Wohnortdaten für die entsprechende Wahrscheinlichkeitsberechnung zu nutzen. Auskunfteien dürfen demnach nicht die potenzielle Zahlungsfähigkeit eines Betroffenen allein aus seiner Wohngegend ableiten, ohne weitere personenbezogene Informationen und Parameter einzubeziehen. Genau ein solches reines Geoscoring sah Caspar in dem Bürgel-Fall gegeben. Die Auskunftei hielt dem Kontrolleur zufolge dagegen, dass sie dem Onlinehändler mitgeteilt habe, der Kunde sei ihr nicht bekannt. Also seien gar keine persönlichen Informationen übermittelt worden. Dieser Einwand überzeugte die Datenschutzaufsicht genauso wenig wie das AG Hamburg. Es bestätigte das Bußgeld in voller Höhe.

Das Urteil ist zwar noch nicht rechtskräftig, da Bürgel Beschwerde dagegen eingelegt hat. Caspar geht trotzdem bereits davon aus, dass er derartige Verfahren künftig gar nicht mehr führen muss. Hintergrund ist, dass die von Mai 2018 an geltende EU-Datenschutz-Grundverordnung die Schranken beim Geoscoring nicht aufhebt, den Bußgeldrahmen aber um ein Vielfaches erhöht (Krempl, Datenschutzverstoß: 15.000 Euro Bußgeld wegen Geoscoring, www.heise.de 26.03.2017; Amtsgericht Hamburg bestätigt Bußgeld gegen Auskunftei, www.datenschutz-hamburg.de 24.03.2017).

Buchbesprechungen



Kühling, Jürgen/Buchner, Benedikt (Hrsg.)
DS-GVO
C.H. Beck München 2017, XVI + 1169 S., 159 €, ISBN 978-3-406-70212-9

Das ist neu. Die Datenschutz-Grundverordnung tritt erst am 25.05.2018 in Kraft und dennoch sind schon eine ganze Reihe juristischer Kommentare angekündigt bzw. schon erschienen. Beginnend mit Plath (Hg.), BDSG/DS-GVO, der der 2. Aufl. 2016 seines BDSG-Kommentars 423 Seiten Kommentierung der DS-GVO hinzufügte und dem Beck'schen Kompakt-Kommentar Paal/Pauly (Hg.), der mit 915 Seiten in kleinerem Format erschien, steht nun ein Jahr vor dem Stichtag bereits ein Großkommentar im Regal: Der Kühling/Buchner. Herausgegeben von Prof. Dr. Jürgen Kühling (Universität Regensburg) und Prof. Dr. Benedikt Buchner (Universität Bremen) sind hier keine Unbekannten am Werk. Um sich geschart haben sie ein illustres Team von weiteren und ebenfalls bestens ausgewiesenen Datenschutzspezialisten aus Universität (Prof. Dr. Bäcker, Mainz; Prof. Dr. Boehm, Karlsruhe; PD Dr. Herbst, Berlin; Prof. Dr. Marschmann, Regensburg; Prof. Dr. Tinnefeld, München), Datenschutzbehörden (Prof. Dr. Caspar, Hamburg; Dr. Dix, Berlin; Dr. Jandt, Kassel; Prof. Dr. Petri, München; Dr. Weichert, Kiel) und Anwaltschaft (Bergt, Berlin; Dr. Hartung, Köln; Dr. Klar, München; Dr. Raab, Nürnberg; Dr. Schröder, Düsseldorf). Herausgekommen ist ein umfangreiches Werk, das das Zeug zum Marktführer hat.

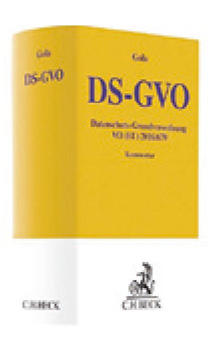
Dass das Datenschutzrecht an literarischer Popularität gewonnen hat, war allerdings schon vorher offenbar, als die Zahl der zum BDSG erschienenen Kommentare den zweistelligen Bereich erreichte. Selbst der nicht-juristische Bereich hat sich – auch beflügelt durch den Nachrichtenkomplex NSA – mit Äußerungen zu datenschutzrechtlichen Fragestellungen überschlagen. Und zu Recht: Ein konsequenter Datenschutz ist Grundvoraussetzung einer demokratischen Gesellschaft (immer noch lesenswert: BVerfGE 65, 1, 43 – Volkszählung). Die Tatsache, dass viele Menschen sich (zum Teil sogar freiwillig und vorsätzlich) wenig darum kümmern, darf nicht daran hindern, den Datenschutz durchzusetzen, weil sich die Gesellschaft sonst nachhaltig zum Schlechten verändert (siehe auch Schirrmacher, Payback 2009 sowie Ego 2013). Ein Recht auf Privatleben ist Grundvoraussetzung für die Entwicklung einer freien und selbstbestimmten Persönlichkeit (Buchner, Art. 1 Rn. 11). Telematiktarife (Rabatte gegen Daten) sind in ihren möglichen Folgen ebenso bedenklich wie die freiwilligen „digitalen Fußfesseln“ (insb. Gesundheits-Apps). Für einige Cent Ersparnis und ein neues Gadget lassen die Kunden zu, dass persönlichste Daten de facto unkontrolliert – weil zumeist im nicht-europäischen

Ausland – und ohne Aussicht auf baldiges Vergessen gesammelt und verarbeitet werden.

Mit fast 1200 Seiten Umfang im großen „roten“ Kommentarformat liegt hier nun ein Buch in der Größe eines Brockhaus-Bandes vor. Und schon beim ersten Schmökern lernt der Rezensent dazu. Der erste Datenschützer war wohl in der Tat Hippokrates, der die ärztliche Schweigepflicht begründete (Weichert, Art. 4 Nr. 15 Rn. 4). Und die heutigen Datenschützer bewirken mit diesem Gesetzeswerk, dass eine Vielzahl von Geschäftsmodellen insbesondere im Online-Sektor „so nicht mehr praktiziert werden können“ (Buchner/Kühling, Art. 7 Rn. 50). Oftmals wird dies allerdings auch schon jetzt gelten – es ist nur nicht durchsetzbar. Es bleibt abzuwarten, wie sich dies ändern wird. Die hiermit im Zusammenhang stehende Frage „Privacy Shield“ wird mit den fortgeschriebenen Problemen ebenfalls einer Antwort harren (Schröder, Art. 45 Rn. 40 ff.). Die aktuellen Äußerungen aus Brüssel lassen für die Zukunft der „Datenbrücke“ keine zwingend guten Prognosen zu.

Manch eine „Kuriosität“ lässt man dem Verordnungsgeber durchgehen, so zum Beispiel die Bemerkung, die Verarbeitung personenbezogener Daten solle „im Dienste der Menschheit stehen“ (EG 4). Eine solche Formulierung findet sich in dieser Deutlichkeit ansonsten eher in Schriften, die die Interessen der datenverarbeitenden Industrie unterstützen sollen. Sie ist im Konjunktiv formuliert richtig, als Leitsatz zu einer Norm zum Schutze des Einzelnen aber wohl nur als Versuch einer Abschwächung zu bewerten. Gemäß EG 2 der RL 95/46 standen Datenverarbeitungssysteme noch „im Dienste des Menschen“, also des jeweilig betroffenen Einzelnen, nicht im noch zu bestimmenden Interesse einer ebenfalls noch zu bestimmenden Mehrheit oder gar im kaum bestimmbaren Interesse „der Menschheit“ insgesamt. Hier sei auf die Gefahr hingewiesen, dass mit vagen oder konkreten Interessen einer Mehrheit der eigentlich intendierte Schutz des Einzelnen ausgehöhlt werden könnte. Es sei die Frage erlaubt, ob diese Formulierung den Auslegungsgrundsätzen zu Art. 8 GRCh entspricht, die in Art. 52 Abs. 1 GRCh niedergelegt sind (dazu Kühling/Raab Einf Rn. 29 ff.).

Man sehe es dem Unterzeichner nach, wenn er der Versuchung nicht widersteht, einzelne Aspekte herauszugreifen, ohne damit die Qualität der übrigen Kommentierung herabzusetzen. Das Buch ist zu umfangreich und zu tiefgehend, um alle Aspekte auf dem beschränkten Raum einer Buchbesprechung angehen zu können. Schließlich gilt: Der Kühling/Buchner hat das Zeug zum Marktführer (Rechtsanwalt Prof. Dr. Stefan Ernst, Freiburg/Br.).



Gola, Peter (Hrsg.)
DS-GVO, Datenschutz-Grundverordnung VO (EU) 2016/679
C.H.Beck 2017, 834 S., ISBN 978 3 406 69543 8, 79,00 €

(tw) Die Strategie des C.H.Beck-Verlags generell bei juristischen Kommentaren und insbesondere auch bei der Kommentierung der Datenschutz-Grundverordnung (DSGVO) ist es, den Markt voll abzudecken und so zu bedienen, dass andere Verlage kaum noch eine Chance haben. Nach dem Schnellschuss (Paal/Pauly, DANA 1/2017, 67) sind inzwischen ein Großkommentar (Kühling/Buchner, s. o.) sowie der (graue) sog. Kurz-Kommentar von Ehmann/Selmayr auf dem Markt. Praktisch zeitgleich erschien der (orangene) „Gola“ in historischer Anknüpfung an die BDSG-Kommentierungen von Gola/Schomerus, die letztmalig 2015 in 12. Auflage erschienen. Dieser relativ preisgünstige Kommentar zielt auf das allgemeine Publikum ab und behandelt die DSGVO-Regelungen zumeist praxisorientierter und vertiefter als der Paal/Pauly. Anders als bisher zum BDSG werden inzwischen die Kommentierungen namentlich zugeordnet, wobei die AutorInnen durchgängig bekannt und qualifiziert sind: Carolyn Eichler, Lorenz Franck, Christoph Klug, Niels Lepperhoff, Alexander Nguyen, Norbert Nolte, Carlo Piltz, Stephan Pötters, Yvette Reif, Sebastian Schulz und Christoph Werkmeister. Diese Kombi verbietet es, den Kommentar in eine bestimmte Ecke zu stellen, da sowohl kritische AufsichtsvertreterInnen und Wissenschaftler wie auch sehr pragmatisch kommentierende Vertreter von Verarbeiterinteressen beteiligt sind. Die Qualität der Kommentierung ist durchgängig erfreulich, so dass ein erster Blick in den „Gola“ insbesondere für die PraktikerIn erkenntnisfördernd ist. Für die wissenschaftliche Tiefe ist dann aber doch noch der Rückgriff auf weitere Literatur nötig, wobei auf diese sehr weitgehend verwiesen wird.

Die Anzahl der Kommentare zur DS-GVO ist zweifellos förderlich für eine intensive Diskussion zu vielen Einzelfragen, die sich um dieses interpretationsbedürftige Regelwerk ergeben und künftig noch lange ergeben werden. Dabei sollte aber nicht nur allein auf den „Gola“ zurückgegriffen werden. So meint z. B. Piltz, dass es zwischen Berufsgeheimnissen und Datenschutzkontrolle einen Konflikt gebe, bei dem erstgenannten der Vorrang gebühre. Diese fatale verfassungs- und europarechtswidrige Ansicht wurde inzwischen durch den Bundesgesetzgeber für Deutschland in Paragrafen gegossen. Oder Gola selbst referiert unkritisch bei Art. 23 die damals noch geplanten und inzwischen etwas relativierten Einschränkungen der Betroffenenrechte. Schulz meint, leider im Einklang mit vielen weiteren Autoren, bei der Auslegung des Art. 22 zum Profiling, dass damit nicht das „Werbescoring“ erfasst würde, womit, entgegen der Intention des europäischen Gesetzgebers, der wichtigste praktische Anwendungsfall des Profiling ins juristische Niemandsland verbannt wird. Dabei wird nicht offengelegt, dass Schulz nicht nur Anwalt ist, sondern auch für den Bundesverband E-Commerce und Versandhandel Deutschland (BEVH) tätig ist, was seine verarbeitungs- und werbefreundliche Auslegung der DSGVO erklärt.

Es ist klar, dass die Auslegung der DSGVO nicht nur ein einträgliches Geschäft, sondern auch der Schlüssel für einträgliche Geschäfte ist. Deshalb muss hierüber öffentlich gestritten werden. Der „Gola“ ist hierfür eine äußerst wertvolle Grundlage.

DatenDebatten

Big Data im Gesundheitswesen



Big Data und E-Health

Herausgegeben von der **Stiftung Datenschutz**

Mit Beiträgen von Prof. Dr. Björn Bergh, Antje Brandner, Prof. Dr. Roland Eils, Prof. Dr. Ulrich M. Gassner, Björn Haferkamp, M.A., Prof. Dr. Dirk Heckmann, Dr. Oliver Heinze, Prof. Dr. Christof von Kalle, Christian Klose, Dr. Ulrike Kutscha, Klaus Müller, Anne Paschke, Bertram Raum, Peter Schaar, Dr. Christopher Schickhardt, Dr. Björn Schreiweis, Prof. Dr. Stefan Selke, Prof. Dr. Stefan Sorgner, Prof. Dr. Frank Ückert, Dr. Thilo Weichert, Prof. Dr. Eva Winkler

2017, 202 Seiten, fester Einband, € (D) 42,–
ISBN 978-3-503-17491-1
DatenDebatten, Band 2

Telemedizin, datenbasierte Gesundheitsanalysen, Health-Apps und mobile Geräte zur individuellen Gesundheitskontrolle – immer mehr Gesundheitsdienstleistungen werden mit Hilfe digitaler Dienste und Strukturen angeboten.

Chancen nutzen, Patientenrechte wahren

Die rasante Entwicklung verspricht nicht nur enorme Qualitätssteigerungen in der Gesundheitsversorgung und neue Märkte im Gesundheitssektor. Sie wirft auch viele Fragen mit weitreichender **Relevanz für den Datenschutz auf**:

- Wie sehen die wissenschaftlichen, aber auch die ökonomischen Perspektiven dieser Entwicklung aus?
- Wie zuverlässig sind digitale Lösungsansätze im Gesundheitsbereich?
- Wie entwickelt sich zukünftig das Arzt-Patienten-Verhältnis?
- Welche gesellschaftlichen Folgen könnte eine „Kultur der Selbstvermessung“ haben?
- Wie kann das Vertrauen der Patienten bzw. der Anwender in E-Health-Dienstleistungen nachhaltig gestärkt werden?

Auch als eBook erhältlich mit komplett verlinkten Inhalts- und Stichwortverzeichnissen.

www.ESV.info/17492

Weitere Informationen:

www.ESV.info/17491



Bestellungen bitte an den Buchhandel oder: Erich Schmidt Verlag GmbH & Co. KG · Genthiner Str. 30 G · 10785 Berlin
Tel. (030) 25 00 85-265 · Fax (030) 25 00 85-275 · ESV@ESVmedien.de · www.ESV.info